

ADDITIVE AVERAGES OF MULTIPLICATIVE CORRELATION SEQUENCES AND APPLICATIONS

SEBASTIÁN DONOSO, ANH N. LE, JOEL MOREIRA, AND WENBO SUN

ABSTRACT. We study sets of recurrence, in both measurable and topological settings, for actions of (\mathbb{N}, \times) and $(\mathbb{Q}^{>0}, \times)$. In particular, we show that autocorrelation sequences of positive functions arising from multiplicative systems have positive additive averages. We also give criteria for when sets of the form $\{(an + b)^\ell / (cn + d)^\ell : n \in \mathbb{N}\}$ are sets of multiplicative recurrence, and consequently we recover two recent results in number theory regarding completely multiplicative functions and the Omega function.

1. INTRODUCTION AND RESULTS

An equation of several variables is *partition regular* if for any finite coloring of \mathbb{N} , there exists a solution to the equation with all variables having the same color. An old question of Erdős and Graham [10] asks whether the equation $x^2 + y^2 = z^2$ is partition regular. A partial answer was obtained in 2016, when the conjecture was confirmed in the case of two colors [15]. In general, the answer to Erdős and Graham's question is still unknown even if we just require two of the variables to have the same color.

Conjecture 1.1. *For any finite coloring of \mathbb{N} , there exist x, y of the same color such that $x^2 + y^2$ (or $x^2 - y^2$) is a perfect square.*

Frantzikinakis and Host proved in [11] that for any finite coloring of \mathbb{N} , there are x, y of the same color such that $16x^2 + 9y^2$ is a perfect square. Expanding on these ideas, the fourth author established an analogue of Conjecture 1.1 where \mathbb{N} is replaced with the ring of integers of a larger number field (see [22, 23]). However the methods used there do not seem to apply to \mathbb{N} .

The above results were proved by first recasting the combinatorial problems into questions in ergodic theory, in particular about sets of return times in multiplicative measure preserving systems. For a semigroup G , a *topological G -system* is a pair (X, T) where X is a compact metric space and T is a G -action on X , i.e. for $g \in G$, $T_g : X \rightarrow X$ is a homeomorphism and for $g, h \in G$, $T_g \circ T_h = T_{gh}$. Let \mathcal{B} be the Borel σ -algebra and μ be a probability measure on

2010 *Mathematics Subject Classification.* Primary: 37B20 ; Secondary: 37A45, 11N37.

The first author was supported by ANID/Fondecyt/1200897 and Centro de Modelamiento Matemático (CMM), ACE210010 and FB210005, BASAL funds for centers of excellence from ANID-Chile.

X such that $\mu(T_g^{-1}A) = \mu(A)$ for all $A \in \mathcal{B}$. Then the tuple (X, \mathcal{B}, μ, T) is called a *measure preserving G -system*. By a *multiplicative measure preserving system*, we mean a measure preserving (\mathbb{N}, \times) -system with \times being the multiplication on \mathbb{N} .

For $x, y \in \mathbb{N}$, $x^2 + y^2$ is a perfect square if and only if $x = k(m^2 - n^2)$ and $y = k(2mn)$ for $k, m, n \in \mathbb{N}$ and $m > n$. Therefore, to answer the case $x^2 + y^2$ of Conjecture 1.1 using the approach in [11], it suffices to solve the following conjecture:

Conjecture 1.2. *Let (X, \mathcal{B}, μ, T) be a measure preserving (\mathbb{N}, \times) -system and $A \in \mathcal{B}$ with $\mu(A) > 0$. There exist $m, n \in \mathbb{N}$ with $m > n$ such that*

$$\mu(T_{m^2-n^2}^{-1}A \cap T_{2mn}^{-1}A) > 0.$$

The idea of using ergodic theoretical methods to solve combinatorial problems traces back to Furstenberg's proof of Szemerédi's Theorem [12] in 1977. The novelty in Frantzikinakis and Host [11]'s approach is the usage of additive averages to study multiplicative measure preserving systems. This idea has the potential to address other unsolved problems in ergodic Ramsey theory regarding partition regularity of polynomial equations and a primary goal of this paper is to begin a systematic study of this new tool and to obtain potential applications.

1.1. Additive averages of multiplicative recurrence sequences. Throughout this paper, for a finite set E and function $f: E \rightarrow \mathbb{C}$, we use $\mathbb{E}_{n \in E} f(n)$ to denote the average $\frac{1}{|E|} \sum_{n \in E} f(n)$. By the von Neumann ergodic theorem, for a multiplicative measure preserving system (X, \mathcal{B}, μ, T) , a set $A \in \mathcal{B}$ with $\mu(A) > 0$ and a multiplicative Følner sequence $(\Phi_N)_{N \in \mathbb{N}}$ in \mathbb{N} (see Section 2 for definitions), we have

$$(1) \quad \lim_{N \rightarrow \infty} \mathbb{E}_{n \in \Phi_N} \mu(A \cap T_n^{-1}A) > 0.$$

On the other hand, it is not clear whether (1) is still true if $(\Phi_N)_{N \in \mathbb{N}}$ is replaced with the additive Følner sequence $([N])_{N \in \mathbb{N}}$. (Here $[N]$ denotes the set $\{1, \dots, N\}$.)

Our first result confirms that this is indeed the case. In fact, we obtain a more general theorem regarding multiple ergodic averages along subsemigroups of (\mathbb{N}, \times) .

Theorem 1.3. *Let (X, \mathcal{B}, μ, T) be a measure preserving (\mathbb{N}, \times) -system and $A \in \mathcal{B}$ with $\mu(A) > 0$. Let G be a subsemigroup of (\mathbb{N}, \times) . Then for every $\ell \in \mathbb{N}$,*

$$\limsup_{N \rightarrow \infty} \mathbb{E}_{n \in G \cap [N]} \mu(A \cap T_n^{-1}A \cap \dots \cap T_{n^\ell}^{-1}A) > 0.$$

Theorem 1.3 follows from the slightly more general Theorem 5.4 below. Besides \mathbb{N} itself, examples of multiplicative semigroups of \mathbb{N} include $\{m^2 + Dn^2 : m, n \in \mathbb{N}\}$ for some $D \in \mathbb{N}$, $\{a^n b^m : m, n \in \mathbb{N}\}$ and $\{m^a n^b q^c : m, n, q \in \mathbb{N}\}$ for $a, b, c \in \mathbb{N}$. We remark that there are two natural ways to take averages along these semigroups. One way is to enumerate its elements

in increasing order as done in Theorem 1.3. Alternatively, one can exploit the fact that these semigroups admit parametrizations and take averages on the parameters. Our next result states that, also with this scheme, the averages of multiple recurrence sequences are positive. To formulate our result we need the notion of *parametrized multiplicative function*, which describes certain parametrizations of multiplicative semigroups. We postpone the formal definition to Section 5.4, but here are some illustrative examples of commutative parametrized multiplicative functions:

- $f: \mathbb{N}^2 \rightarrow \mathbb{N}$ defined by $f(n_1, n_2) = n_1^2 + Dn_2^2$, for any $D \in \mathbb{N}$,
- $f: \mathbb{N}^2 \rightarrow \mathbb{N}$ defined by $f(n_1, n_2) = |n_1^2 + n_1n_2 - n_2^2|$,
- $f: \mathbb{N}^3 \rightarrow \mathbb{N}$ defined by $f(n_1, n_2, n_3) = n_1^{a_1}n_2^{a_2}n_3^{a_3}$ for any $a_1, a_2, a_3 \in \mathbb{N}$.

Theorem 1.4. *Let (X, \mathcal{B}, μ, T) be a measure preserving (\mathbb{N}, \times) -system and $A \in \mathcal{B}$ with $\mu(A) > 0$. Let $f: \mathbb{N}^k \rightarrow \mathbb{N}$ be a commutative parametrized multiplicative function and $\ell \in \mathbb{N}$. Then*

$$\liminf_{N \rightarrow \infty} \mathbb{E}_{n \in [N]^k} \mu \left(A \cap T_{f(n)}^{-1} A \cap T_{f(n)^2}^{-1} A \cap \cdots \cap T_{f(n)^\ell}^{-1} A \right) > 0.$$

Theorem 1.4 follows from the more general Theorem 5.16 in Section 5. As an illustrative special case of Theorem 1.4 we obtain

Proposition 1.5. *Let (X, \mathcal{B}, μ, T) be a measure preserving (\mathbb{N}, \times) -system and let $A \in \mathcal{B}$ with $\mu(A) > 0$. Then*

$$\liminf_{N \rightarrow \infty} \mathbb{E}_{m, n \in [N]} \mu(A \cap T_{m^2+n^2}^{-1} A) > 0.$$

1.2. Topological recurrence and applications to number theory. A subset R of the set of positive rational numbers $\mathbb{Q}^{>0}$ is called a *set of (measurable) multiplicative recurrence* if for every $(\mathbb{Q}^{>0}, \times)$ -system (X, \mathcal{B}, μ, T) and $A \in \mathcal{B}$ with $\mu(A) > 0$, there exists $r \in R$ for which $\mu(A \cap T_r^{-1} A) > 0$. By Furstenberg's correspondence principle, R is a set of multiplicative recurrence if and only if for any $E \subset \mathbb{N}$ of positive upper multiplicative density (see Section 2 for definitions), there exist $x, y \in E$ such that $x/y \in R$. If Conjecture 1.2 is true, then it follows that $\{(m^2 - n^2)/(2mn) : m, n \in \mathbb{N}, m > n\}$ is a set of multiplicative recurrence.

There is a weaker notion that suffices for our purpose of studying partition regularity called sets of topological multiplicative recurrence. A set $R \subset \mathbb{Q}^{>0}$ is called a *set of topological multiplicative recurrence* if for every minimal topological $(\mathbb{Q}^{>0}, \times)$ -system (X, T) and $U \subset X$ open and non-empty, there exists $r \in R$ such that $U \cap T_r^{-1} U \neq \emptyset$. It turns out that R is a set of topological multiplicative recurrence if and only if for any finite coloring of \mathbb{N} , there exist x, y of the same color such that $x/y \in R$ (see Proposition 2.13 below).

In Section 2 we show that if $\phi: (\mathbb{N}, +) \rightarrow (\mathbb{Q}^{>0}, \times)$ is a homomorphism and $S \subset \mathbb{N}$ is a set of topological (or measurable) additive recurrence, then $\phi(S)$ is a set of topological (or measurable) multiplicative recurrence. Using this fact, and drawing on the many known

examples of sets of additive recurrence (cf. [12, 16, 20]), one can exhibit examples of sets of multiplicative recurrence: $\{2^{P(n)} : n \in \mathbb{N}\}$ where $P \in \mathbb{Z}[x]$ satisfies $P(0) = 0$ and $\{2^{p-1} : p \text{ prime}\}$. However, all such examples are confined to a sparse semigroup of the form $\{a^n : n \in \mathbb{N}\}$, and there are hardly any other known examples of sets of multiplicative recurrence. Our next result produces a set of multiplicative recurrence which does not belong to the aforementioned class.

Theorem 1.6. *Let $a, c, \ell \in \mathbb{N}$, $b, d \in \mathbb{Z}$ and let $R := \left\{ \left(\frac{an+b}{cn+d} \right)^\ell : n \in \mathbb{N} \right\}$.*

- (1) *If $a \neq c$, then R is not a set of topological multiplicative recurrence.*
- (2) *If $a = c$, $b \neq d$ and there exists a prime p such that $p|a$ but $p \nmid bd$, then R is not a set of topological multiplicative recurrence.*
- (3) *If $a = c$ and either $a|b$ or $a|d$, then R is a set of topological multiplicative recurrence.*

¹

Theorem 1.6 follows from combining Propositions 3.2, 3.3 and 3.6.

A function $f: \mathbb{N} \rightarrow \mathbb{C}$ is called *completely multiplicative* if $f(mn) = f(m)f(n)$ for $m, n \in \mathbb{N}$. Klurman and Mangerel [17] proved that for any completely multiplicative function f with $|f(n)| = 1$ for $n \in \mathbb{N}$, one has $\liminf_{n \rightarrow \infty} |f(n+1) - f(n)| = 0$. They remarked that their proof can be modified to treat the case in which the shift 1 is replaced by any fixed $k \in \mathbb{N}$. As an application of Theorem 1.6, we give a strengthening of their result by allowing both arbitrary shifts and dilations.

Corollary 1.7. *Let $f: \mathbb{N} \rightarrow \mathbb{C}$ be a completely multiplicative function with $|f(n)| = 1$ for $n \in \mathbb{N}$. Then for all $a, k \in \mathbb{N}$,*

$$\liminf_{n \rightarrow \infty} |f(an+k) - f(an)| = 0.$$

The proof of Corollary 1.7 is given in Section 3, after the proof of Proposition 3.6. In the previous corollary, by setting $f = \xi^{\Omega(n)}$, where ξ is a q -th root of 1 and, for $n \in \mathbb{N}$, $\Omega(n)$ is the number of prime factors of n counting with multiplicity, one immediately derives the following enhancement of [17, Corollary 1.3].

Corollary 1.8. *For any $a, q, k \in \mathbb{N}$, there exists infinitely many $n \in \mathbb{N}$ such that $\Omega(an+k) \equiv \Omega(an) \pmod{q}$.*

Using (an appropriate version of) the Poincaré recurrence theorem it can be shown that every subsemigroup of $(\mathbb{Q}^{>0}, \times)$ is a set of multiplicative recurrence. Therefore, to understand which algebraic sets are sets of multiplicative recurrence, one needs to know which contain a

¹In the special case $\ell = a = c = 1$ and $b = d = 0$, this result was also observed by Bergelson in [2, Section 5].

subsemigroup. Our next theorem characterizes all polynomials of integer coefficients whose images contain subsemigroups of $(\mathbb{Q}^{>0}, \times)$.

Theorem 1.9. *For $P \in \mathbb{Z}[x]$, the set $\{P(n) : n \in \mathbb{N}\}$ contains an infinite subsemigroup of $(\mathbb{Q}^{>0}, \times)$ if and only if $P(x) = (ax + b)^d$ for some $a, d \in \mathbb{N}$, $b \in \mathbb{Z}$ with $a|b(b - 1)$.*

Theorem 1.9 follows from the more general Theorem 4.3.

Regarding linear polynomials, we show that containing subsemigroups is not only a sufficient but also a necessary condition for their images to be sets of multiplicative recurrence.

Theorem 1.10. *For every $a, b \in \mathbb{N}$, $\{an + b : n \in \mathbb{N}\}$ is a set of multiplicative recurrence if and only if $a|b(b - 1)$.*

Theorem 1.10 is implied by Theorem 3.8 in Section 3.

Lastly, as previously mentioned, it is unknown whether the sets arising from Pythagorean triples are sets of multiplicative recurrence. However, we show that these sets do not contain subsemigroups of $(\mathbb{Q}^{>0}, \times)$.

Proposition 1.11. *Neither of the sets*

$$\left\{ \frac{m^2 + n^2}{2mn} : m, n \in \mathbb{N} \right\} \quad \text{and} \quad \left\{ \frac{2mn}{m^2 - n^2} : m, n \in \mathbb{N}, m > n \right\}$$

contain an infinite subsemigroup of $(\mathbb{Q}^{>0}, \times)$.

Proposition 1.11 is proved in Section 4, after Lemma 4.4.

Organization of the paper. In Section 2 we give the background regarding sets of multiplicative recurrence in both topological and measurable settings. Section 3 is devoted to studying the topological recurrence properties of certain algebraic sets and providing applications in number theory. In particular, Theorem 1.6, Corollary 1.7, Corollary 1.8 and Theorem 1.10 are proved in this section. In Section 4, we analyze polynomial configurations and investigate when the image of \mathbb{N} under a polynomial map contains a semigroup of (\mathbb{N}, \times) . Section 5 contains the ergodic theoretical point of view of this article where Theorem 1.3 and Theorem 1.4 will be proved. Finally, in Section 6, we study the problem of finding Pythagorean pairs and triples in dense subsets of finite fields.

Acknowledgements. We thank Florian Richter for help with the proof of Lemma 3.5 and thank Vitaly Bergelson for helpful conversations. We also thank the referee for suggestions that improve the organization and readability of the paper.

2. BACKGROUND

In this section we collect basic facts about sets of recurrence for the semigroup (\mathbb{N}, \times) of natural numbers and the semigroup $(\mathbb{Q}^{>0}, \times)$ of positive rational numbers, both under multiplication. Most of the content is well known and presented here for completeness.

Notations. In this article, $\mathbb{N} = \{1, 2, \dots\}$ denotes the set of positive natural numbers, and $\mathbb{Q}^{>0}$ denotes the set of positive rational numbers. For a positive natural number N , we let $[N]$ denote the set $\{1, \dots, N\}$.

2.1. Multiplicatively invariant density and Furstenberg's correspondence. A *Følner sequence* in a countable semigroup G is a sequence $\Phi = (\Phi_N)_{N \in \mathbb{N}}$ of finite subsets of G which are asymptotically invariant in the sense that for any $g \in G$,

$$\lim_{N \rightarrow \infty} \frac{|g\Phi_N \cap \Phi_N|}{|\Phi_N|} = 1,$$

where $g\Phi_N = \{gx : x \in \Phi_N\}$. Given a Følner sequence Φ on a semigroup G , the *upper density* of a set $A \subset G$ with respect to Φ is the quantity

$$\bar{d}_\Phi(A) := \limsup_{N \rightarrow \infty} \frac{|A \cap \Phi_N|}{|\Phi_N|}.$$

For a subset $A \subset G$ of a semigroup G and an element $g \in G$, we write $S/g := \{x \in G : xg \in A\}$. It is easy to check from the definition that $\bar{d}_\Phi(A/g) = \bar{d}_\Phi(A)$ for any $g \in G$.

The *upper Banach density* of A is $d^*(A) := \sup_\Phi \bar{d}_\Phi(A)$, where the supremum is taken over all Følner sequences Φ on G . This supremum is always achieved, so for each set A there is a Følner sequence Φ such that $d^*(A) = \bar{d}_\Phi(A)$.

A discussion of Følner sequences and invariant densities in the case where $G = (\mathbb{N}, \times)$ is provided in [4]. As a concrete example one can take the sequence $\Phi_N := \{x \in \mathbb{N} : x|N!\}$, but the exact choice will not be important in our discussion. Note that any Følner sequence for (\mathbb{N}, \times) is also a Følner sequence for $(\mathbb{Q}^{>0}, \times)$.

Given a semigroup G , a *measure preserving G -system* is a measure preserving system (X, \mathcal{B}, μ, T) where (X, \mathcal{B}, μ) is a probability space and $T = (T_g)_{g \in G}$ is an action of G on X by measure preserving transformations $T_g : X \rightarrow X$ which satisfy $T_{gh} = T_g \circ T_h$ for every $g, h \in G$.

The Furstenberg correspondence principle connects sets with positive upper density and measure preserving systems. Here is the version we will use. Given a subset E of a semigroup G and $n \in G$ we let E/n denote $\{m \in G : mn \in E\}$.

Theorem 2.1 (Furstenberg's correspondence principle for semigroups, cf. [5, Theorem 5.8 and Remark 5.9]). *Let G be a countable commutative semigroup, let $E \subset \mathbb{N}$ and let Φ be*

a Følner sequence in G . Then there exists a G -system (X, \mathcal{B}, μ, T) and a set $A \in \mathcal{B}$ with $\mu(A) = \bar{d}_\Phi(E)$ and, for every $n_1, \dots, n_k \in G$,

$$\bar{d}_\Phi(E \cap (E/n_1) \cap (E/n_2) \cap \dots \cap (E/n_k)) \geq \mu(A \cap T_{n_1}^{-1}A \cap \dots \cap T_{n_k}^{-1}A).$$

2.2. Syndetic sets. A subset $S \subset G$ is called (*right*) *syndetic* if there exists a finite set $F \subset G$ such that $S/F := \bigcup_{x \in F} S/x = G$. The following proposition is well known and we include its proof for completeness.

Proposition 2.2. *A set S is syndetic if and only if it has positive upper density with respect to any Følner sequence.*

Proof. If S is syndetic and Φ is a Følner sequence, then take F finite so that $S/F = G$. We have $1 = \bar{d}_\Phi(G) \leq \sum_{x \in F} \bar{d}_\Phi(S/x) = \bar{d}_\Phi(S) \cdot |F|$, so $\bar{d}_\Phi(S) > 0$.

Conversely, if S is not syndetic and Φ is a Følner sequence, for every $N \in \mathbb{N}$ we have that $S/\Phi_N \neq G$. Take $x_N \in G \setminus (S/\Phi_N)$. Then $\Psi_N := x_N \Phi_N$ is disjoint from S . On the other hand, the sequence $\Psi = (\Psi_N)_{N \in \mathbb{N}}$ is a Følner sequence, and so $\bar{d}_\Psi(S) = 0$. \square

In order to prove Theorem 1.3, we will need the following theorem of Furstenberg and Katznelson [14] (see also [4, Page 9]). Recall that a commutative semigroup is *cancelative* if and only if it is a subsemigroup of a group.

Theorem 2.3 (Furstenberg-Katznelson [14]). *Let G be a cancelative commutative semigroup and let T_1, \dots, T_ℓ be commuting measure preserving actions of G on the probability space (X, \mathcal{B}, μ) . Then for every $A \in \mathcal{B}$ with $\mu(A) > 0$, there exist $\delta > 0$ and a syndetic set $S \subset G$ such that for every $g \in S$,*

$$\mu(A \cap T_{1,g}^{-1}A \cap \dots \cap T_{\ell,g}^{-1}A) > \delta.$$

When $\ell = 1$, Theorem 2.3 becomes significantly simpler and is a version of Khintchine's recurrence theorem. It turns out that, in this case, it is possible to extend the scope of Theorem 2.3 by dropping the assumption that G is cancelative and commutative. This result is probably well known; we provide a short proof which is almost verbatim taken from the proof of [2, Theorem 5.1].

Theorem 2.4 (Khintchine's theorem). *Let G be a countable semigroup, let $(T_g)_{g \in G}$ be an action of G by measure preserving transformations on a probability space (X, \mathcal{B}, μ) and let $A \in \mathcal{B}$ with $\mu(A) > 0$. Then for every $\epsilon > 0$ the set*

$$R := \{g \in G : \mu(A \cap T_g^{-1}A) > \mu^2(A) - \epsilon\}$$

is syndetic.

Proof. Suppose, for the sake of a contradiction that R is not syndetic. Choose $g_1 \in G \setminus R$ arbitrary. Then, inductively, for each $m \geq 1$ let $F_m = \{g_m g_{m-1} \cdots g_n : 1 \leq n \leq m\}$ and choose $g_{m+1} \in G \setminus R F_m^{-1}$. This is possible if R is not syndetic. From the construction we have $F_m = g_m F_{m-1} \cup \{g_m\}$, and hence it follows that $F_m \cap R \subset \{g_m\}$ for every $m \in \mathbb{N}$.

Let $N \in \mathbb{N}$ be large, to be determined later depending only on $\mu(A)$ and ϵ and let $f = \frac{1}{N} \sum_{n=1}^N 1_A \circ T_{g_n g_{n-1} \cdots g_1}$. Clearly $\int_X f \, d\mu = \mu(A)$. By the Cauchy-Schwarz inequality,

$$\begin{aligned} \mu(A)^2 &\leq \int_X f^2 \, d\mu = \frac{1}{N^2} \sum_{n,m=1}^N \mu(T_{g_n g_{n-1} \cdots g_1}^{-1} A \cap T_{g_m g_{m-1} \cdots g_1}^{-1} A) \\ &= \frac{1}{N^2} \left(\sum_{n=1}^N \mu(A) + 2 \sum_{m=2}^N \sum_{n=1}^{m-1} \mu(T_{g_n g_{n-1} \cdots g_1}^{-1} A \cap T_{g_m g_{m-1} \cdots g_1}^{-1} A) \right) \\ &= \frac{1}{N^2} \left(N\mu(A) + 2 \sum_{m=2}^N \sum_{n=1}^{m-1} \mu(A \cap T_{g_m g_{m-1} \cdots g_{n+1} g_n}^{-1} A) \right) \\ &= \frac{1}{N} \mu(A) + \frac{2}{N^2} \left(\sum_{m=2}^N \sum_{g \in F_m} \mu(A \cap T_g^{-1} A) \right) \\ &\leq \frac{1}{N} \mu(A) + \frac{2}{N^2} \binom{N}{2} (\mu^2(A) - \epsilon) \end{aligned}$$

which is a contradiction if N is large enough. \square

2.3. Sets of multiplicative recurrence. Sets of recurrence for $(\mathbb{Z}, +)$ -systems, and their connection to combinatorics were introduced by Furstenberg in his book [13]. Sets of recurrence for arbitrary countable semigroups were defined and studied in [7], and the specific case when the semigroup is (\mathbb{N}, \times) in [4].

Definition 2.5 (Cf. [7, Definition 1.1]). Let G be a semigroup and let $R \subset G$. We say that R is a *set of recurrence*, or a *set of measurable recurrence* if for any measure preserving action $T = (T_g)_{g \in G}$ of G on a probability space (X, μ) and any $A \subset X$ with $\mu(A) > 0$ there exists $r \in R$ such that $\mu(A \cap T_r^{-1} A) > 0$.

Examples of sets of recurrence include G itself and any subsemigroup of G . In particular, note that if G admits an identity e , then the singleton $\{e\}$ is a set of recurrence. More generally, the usual proof of Poincaré's recurrence theorem can be adapted to show that any Δ -set (i.e., a set of the form $\{g_i g_{i+1} \cdots g_j : i \leq j\}$ for some sequence $(g_i)_{i \in \mathbb{N}}$ in G) is a set of recurrence.

Proposition 2.6. *Let G, H be semigroups and let $\phi : G \rightarrow H$ be a homomorphism. If $R \subset G$ is a set of recurrence, then $\phi(R)$ is a set of recurrence in H .*

Proof. Composing any measure preserving action of H with ϕ yields a measure preserving action of G on the same space, and the conclusion follows. \square

We are mainly interested in the semigroup (\mathbb{N}, \times) . In view of the following lemma, we will also consider the group $(\mathbb{Q}^{>0}, \times)$. We denote by $d_{\times}^*(A)$ the Banach upper density of A with respect to the multiplicative structure in either (\mathbb{N}, \times) or $(\mathbb{Q}^{>0}, \times)$.

The following proposition is well known among experts but we were unable to find a complete proof in the literature.

Proposition 2.7. *Let $R \subset \mathbb{Q}^{>0}$. Then the followings are equivalent:*

- (1) *R is a set of recurrence, i.e., for any measure preserving action T of $(\mathbb{Q}^{>0}, \times)$ on a probability space (X, μ) and any $A \subset X$ with $\mu(A) > 0$ there exists $r \in R$ such that $\mu(A \cap T_r^{-1}A) > 0$.*
- (2) *For any measure preserving action T of (\mathbb{N}, \times) on a probability space (X, μ) and any $A \subset X$ with $\mu(A) > 0$ there exists $a, b \in \mathbb{N}$ with $a/b \in R$ such that $\mu(T_a^{-1}A \cap T_b^{-1}A) > 0$.*
- (3) *For any $A \subset \mathbb{Q}^{>0}$ with $d_{\times}^*(A) > 0$ there exists $r \in R$ such that $A \cap A/r \neq \emptyset$.*
- (4) *For any $A \subset \mathbb{Q}^{>0}$ with $d_{\times}^*(A) > 0$ there exists $r \in R$ such that $d_{\times}^*(A \cap A/r) > 0$.*
- (5) *For any $A \subset \mathbb{N}$ with $d_{\times}^*(A) > 0$ there exist $a, b \in \mathbb{N}$ with $a/b \in R$ such that $A/a \cap A/b \neq \emptyset$.*
- (6) *For any $A \subset \mathbb{N}$ with $d_{\times}^*(A) > 0$ there exists $a, b \in \mathbb{N}$ with $a/b \in R$ such that $d_{\times}^*(A/a \cap A/b) > 0$.*

Proof. The implications (6) \Rightarrow (5) and (4) \Rightarrow (3) are trivial. The implications (1) \Rightarrow (4) and (2) \Rightarrow (6) follow directly from the Furstenberg correspondence principle, Theorem 2.1.

The implications (3) \Rightarrow (1) and (5) \Rightarrow (2) have very similar proofs, based on an observation of Bergelson, so here we only give the proof of (5) \Rightarrow (2). Suppose we are given a measure preserving action T of (\mathbb{N}, \times) on a probability space (X, μ) and a set $A \subset X$ with $\mu(A) > 0$. Applying [4, Theorem 3.14] we find a set $P \subset \mathbb{N}$ with $d_{\times}^*(P) > 0$ and such that for any $a, b \in P$, $\mu(T_a^{-1}A \cap T_b^{-1}A) > 0$. Using (5) we can then find $a, b \in P$ with $a/b \in R$, establishing (2).

The implication (2) \Rightarrow (1) follows from the fact that any measure preserving action of $(\mathbb{Q}^{>0}, \times)$ induces a natural measure preserving action of the subsemigroup (\mathbb{N}, \times) . Finally, the implication (1) \Rightarrow (2) follows from a routine inverse extension argument, which we provide for completeness.

Let $(T_n)_{n \in \mathbb{N}}$ be a measure preserving action of (\mathbb{N}, \times) on (X, μ) . The invertible extension of the measure preserving system $(X, \mu, (T_n)_{n \in \mathbb{N}})$ is the system $(Y, \nu, (S_u)_{u \in \mathbb{Q}^{>0}})$ where

$$Y = \left\{ (x_u)_{u \in \mathbb{Q}^{>0}} \in X^{\mathbb{Q}^{>0}} : (\forall n \in \mathbb{N})(\forall u \in \mathbb{Q}^{>0}) x_{un} = T_n x_u \right\},$$

$S_\nu(x_u)_{u \in \mathbb{Q}^{>0}} = (x_{uv})_{u \in \mathbb{Q}^{>0}} \subset X^{\mathbb{Q}^{>0}}$ and for any cylinder set $C = \prod_{u \in F} A_u \times \prod_{u \in \mathbb{Q}^{>0} \setminus F} X$ where $F \subset \mathbb{Q}^{>0}$ is finite and $A_u \subset X$ are arbitrary measurable sets we have $\nu(C) = \mu(\bigcap_{u \in F} T_{un}^{-1} A_u)$, where $n \in \mathbb{N}$ is any common denominator of all elements of F . It is routine to check that $(Y, \nu, (S_u)_{u \in \mathbb{Q}^{>0}})$ is indeed a measure preserving system, and that the projection defined by $(x_u)_{u \in \mathbb{Q}^{>0}} \mapsto x_1$ is a factor map between the (\mathbb{N}, \times) systems $(Y, \nu, (S_u)_{u \in \mathbb{N}})$ and $(X, \mu, (T_n)_{n \in \mathbb{N}})$. On the other hand, the fact that (1) holds for the system $(Y, \nu, (S_u)_{u \in \mathbb{Q}^{>0}})$ implies that (2) holds for the system $(Y, \nu, (S_u)_{u \in \mathbb{N}})$. But the property (2) passes through to factors, so it also holds for the original system $(X, \mu, (T_n)_{n \in \mathbb{N}})$. \square

A weaker notion of recurrence is *topological recurrence*, which we now define. Given a semigroup G , a *topological G -system* is a pair (X, T) where X is a compact metric space and $T = (T_g)_{g \in G}$ is an action of G on X via continuous functions. A topological G -system is *minimal* if every orbit $\text{orb}(x, T) := \{T_g x : g \in G\}$ is dense in X .

Definition 2.8. Let G be a semigroup and let $R \subset G$. We say that R is a *set of topological recurrence* if for any minimal G -system and any non-empty open set $U \subset X$ there exists $r \in R$ such that $U \cap T_r^{-1} U \neq \emptyset$.

One can not drop the minimality condition entirely in this definition, as otherwise no set R would satisfy it. However, it is possible to slightly relax the minimality condition and still have an equivalent definition. Recall that given a topological G -system (X, T) , a point $x \in X$ is called a *minimal point* if its orbit closure $\overline{\text{orb}(x, T)}$ is minimal.

Proposition 2.9. *Let G be a semigroup and let $R \subset G$. Then R is a set of topological recurrence if and only if for any topological G -system (X, T) with a dense set of minimal points, and any non-empty open set $U \subset X$ there exists $r \in R$ such that $U \cap T_r^{-1} U \neq \emptyset$.*

Proof. Let $x \in U$ be a minimal point, let $Y = \overline{\text{orb}(x, T)}$ and let $V := Y \cap U \neq \emptyset$. Then (Y, T) is a minimal system and V a non-empty open subset of Y , so there exists $r \in R$ such that $V \cap T_r^{-1} V \neq \emptyset$, which implies that $U \cap T_r^{-1} U \neq \emptyset$. \square

If G is amenable (in particular if G is commutative) then in view of Bogolyubov-Krilov's theorem [8], every set of recurrence is a set of topological recurrence. We remark in passing that this is not true in general for non-amenable semigroups, and in fact Bergelson conjectures that it is never true for non-amenable groups (cf. [6] or [3, Conjecture after Exercise 20]).

One can also ask whether every set of topological recurrence is a set of measurable recurrence. When $G = (\mathbb{N}, +)$, a negative answer was given by Kriz [18]. We show below that we can use Kriz's example to answer the question in the negative for the semigroup (\mathbb{N}, \times) .

Proposition 2.10. *Let G, H be commutative semigroups and let $\phi : G \rightarrow H$ be a homomorphism. If $R \subset G$ is a set of topological recurrence, then $\phi(R)$ is a set of topological recurrence in H .*

Proof. Let T be a minimal continuous action of H on the compact metric space X and let $U \subset X$ be open and non-empty. Let S be the G -action on X defined by $S_g = T_{\phi(g)}$, let $x \in U$, let $Y_0 := \overline{\{S_g x : g \in G\}}$ and let $Y \subset Y_0$ be a minimal S -subsystem. Since T is minimal, there exists $h \in H$ such that $V := T_h^{-1}U \cap Y \neq \emptyset$.

The set V is a non-empty open subset of Y , so by the hypothesis there exists $g \in R$ such that $S_g^{-1}V \cap V \neq \emptyset$. This implies that $S_g^{-1}T_h^{-1}U \cap T_h^{-1}U \neq \emptyset$, and hence $T_{\phi(g)}^{-1}U \cap U \neq \emptyset$ as well. \square

Corollary 2.11. *There exists $R \subset \mathbb{N}$ which is a set of topological recurrence in (\mathbb{N}, \times) but not a set of measurable recurrence in (\mathbb{N}, \times) .*

Proof. Let $R \subset \mathbb{N}$ be a set of additive topological recurrence which is not a set of additive recurrence. Let $\phi : \mathbb{N} \rightarrow \mathbb{N}$ be the map $\phi(n) = 2^n$. Observe that $\phi : (\mathbb{N}, +) \rightarrow (\mathbb{N}, \times)$ is a homomorphism, so in view of Proposition 2.10 the set $\phi(R)$ is a set of multiplicative topological recurrence.

Let (X, μ, T) be an additive measure preserving system, and $A \subset X$ satisfy $\mu(A) > 0$ but $\mu(A \cap T^{-n}A) = 0$ for all $n \in R$. Consider the multiplicative measure preserving action S on (X, μ) given by $S_n = T^{a(n)}$, where $a(n)$ is the unique integer such that $n = 2^{a(n)}b(n)$, with $b(n)$ odd. Since $a(\phi(n)) = n$ for all $n \in \mathbb{N}$, it follows that $\mu(S_m^{-1}A \cap A) = 0$ for all $m \in \phi(R)$, and hence that $\phi(R)$ is not a set of multiplicative recurrence. \square

Remark 2.12. We note that in general, shifts and dilations of sets of measurable multiplicative recurrence are not sets of measurable or even topological multiplicative recurrence. For example, $\{4^n : n \in \mathbb{N}\}$ is a set of multiplicative recurrence since it is a semigroup. On the other hand, $\{4^n + 3 : n \in \mathbb{N}\}$ is not since it is contained in $4\mathbb{N} + 3$ and it is shown in Theorem 1.10 that the latter set is not a set of topological multiplicative recurrence. For dilations, the set $\{3 \cdot 4^n : n \in \mathbb{N}\}$ is not a set of multiplicative recurrence as seen in the following coloring: For $n \in \mathbb{N}$, write $n = 3^k q$ where $k \in \mathbb{N} \cup \{0\}$ and $q \in \mathbb{N}$ with $3 \nmid q$. Then color $c(n) = 0$ if k is even and $c(n) = 1$ if k is odd.

Proposition 2.13. *Let $R \subset \mathbb{Q}^{>0} \setminus \{1\}$. Then the followings are equivalent:*

- (1) *R is a set of topological recurrence, i.e. for any minimal action T of $(\mathbb{Q}^{>0}, \times)$ on a compact metric space X and any non-empty open set $U \subset X$ there exists $r \in R$ such that $U \cap T_r^{-1}U \neq \emptyset$.*
- (2) *For any topological $(\mathbb{Q}^{>0}, \times)$ -system (X, T) with a dense set of minimal points and any non-empty open set $U \subset X$ there exist infinitely many $r \in R$ such that $U \cap T_r^{-1}U \neq \emptyset$.*

- (3) For any minimal action T of $(\mathbb{N}^{>0}, \times)$ on a compact metric space X and any non-empty open set $U \subset X$ there exist infinitely many pairs $(a, b) \in \mathbb{N}^2$ with $a/b \in R$ such that $T_a^{-1}U \cap T_b^{-1}U \neq \emptyset$.
- (4) For any finite partition $\mathbb{Q}^{>0} = C_1 \cup \dots \cup C_s$ there exists $i \in \{1, \dots, s\}$, $r \in R$ such that $C_i \cap C_i/r \neq \emptyset$.
- (5) For any finite partition $\mathbb{N} = C_1 \cup \dots \cup C_s$ there exist $i \in \{1, \dots, s\}$, $a, b \in \mathbb{N}$ with $a/b \in R$ such that $C_i \cap C_i/r \neq \emptyset$.

Moreover, any of the conditions from Proposition 2.7 implies any of the conditions from this lemma.

Proof. Similar to Proposition 2.7, the proof Proposition 2.13 is routine, with the exception of the implication (1) \Rightarrow (3), which we prove here. Given a minimal multiplicative topological system $(X, (T_n)_{n \in \mathbb{N}})$, let $(Y, (S_u)_{u \in \mathbb{Q}^{>0}})$ be its invertible extension, defined so that

$$Y = \left\{ (x_u)_{u \in \mathbb{Q}^{>0}} \in X^{\mathbb{Q}^{>0}} : (\forall n \in \mathbb{N})(\forall u \in \mathbb{Q}^{>0})x_{un} = T_n x_u \right\} \subset X^{\mathbb{Q}^{>0}}$$

and $S_v(x_u)_{u \in \mathbb{Q}^{>0}} = (x_{uv})_{u \in \mathbb{Q}^{>0}}$. Given a cylinder set $C = \prod_{u \in F} A_u \times \prod_{u \in \mathbb{Q}^{>0} \setminus F} X \subset X^{\mathbb{Q}^{>0}}$, where $F \subset \mathbb{Q}^{>0}$ is finite and $A_u \subset X$ are open sets, we have $C \cap Y \neq \emptyset$ if and only if $\bigcap_{u \in F} T_{un}^{-1} A_u \neq \emptyset$, where $n \in \mathbb{N}$ is any common denominator of all elements of F . For any such C and any $x \in Y$, since (X, T) is minimal the orbit of x_{n-1} is dense in X under T and hence for some $m \in \mathbb{N}$ we have $T_m x_{n-1} \in \bigcap_{u \in F} T_{un}^{-1} A_u$ so that $T_{nm} x_{n-1} \in A_u$ for all $u \in F$. Since $x \in Y$ and $nm \in \mathbb{N}$, we have that $T_{nm} x_{n-1} = x_{nm}$, and hence $(S_m x)_u = x_{mu} \in A_u$ for all $u \in F$. We conclude that $(Y, (S_m)_{m \in \mathbb{N}})$ is also a minimal (\mathbb{N}, \times) system. Since the projection defined by $(x_u)_{u \in \mathbb{Q}^{>0}} \mapsto x_1$ is a factor map between $(Y, (S_m)_{m \in \mathbb{N}})$ and (X, T) , the property (3) passes through to factors, and the property (1) for $(Y, (S_u)_{u \in \mathbb{Q}^{>0}})$ implies property (3) for $(Y, (S_m)_{m \in \mathbb{N}})$, this finishes the proof. \square

We remark in passing that items (4) and (6) of Proposition 2.7 also have an analogue for topological recurrence, using the notion of piecewise syndetic set.

Corollary 2.14. *Let $\ell \in \mathbb{N}$. A set $R \subset \mathbb{Q}^{>0}$ is a set of topological multiplicative recurrence if and only if $R' = \{r^\ell : r \in R\}$ is a set of topological multiplicative recurrence.*

Proof. Suppose $R \subset \mathbb{Q}^{>0}$ is a set of topological multiplicative recurrence. In view of Proposition 2.10, we have R' is a set of topological multiplicative recurrence.

Now let R be such that $R' = \{r^\ell : r \in R\}$ is a set of topological multiplicative recurrence. Letting χ be a finite coloring of \mathbb{N} , we claim that there are $x, y \in \mathbb{N}$ with $\chi(x) = \chi(y)$ and $x/y \in R$. Consider the coloring $\tilde{\chi}$ defined as follows: for any $x \in \mathbb{N}$, write $x = y_x^\ell z_x$ where $y_x, z_x \in \mathbb{N}$ and z_x is not divisible by any ℓ -th power. (Note that y_x and z_x are uniquely determined by x .) Then for such x , define $\tilde{\chi}(x) = \chi(y_x)$. Since R' is a set of topological

multiplicative recurrence, there exist $a, b \in \mathbb{N}$ such that $\tilde{\chi}(a) = \tilde{\chi}(b)$ and $a/b = r^\ell$ for some $r \in R$. By writing $a = y_a^\ell z_a$ and $b = y_b^\ell z_b$, we have that $r^\ell = a/b = (y_a/y_b)^\ell \cdot z_a/z_b$. Since z_a and z_b are not divisible by any ℓ -th power, it follows that $z_a = z_b$ and $y_a/y_b = r$. Moreover, $\chi(y_a) = \tilde{\chi}(a) = \tilde{\chi}(b) = \chi(y_b)$. Hence, $\chi(y_a) = \chi(y_b)$ and $y_a/y_b \in R$; so our proof finishes. \square

3. SETS OF MULTIPLICATIVE RECURRENCE AND APPLICATIONS

3.1. Rational functions. The purpose of this section is to prove Theorem 1.6. We start with the following necessary criteria for a set to be a set of topological multiplicative recurrence.

Lemma 3.1. *For any $\epsilon, M \in \mathbb{R}$ satisfying $0 < \epsilon < 1 < 1 + \epsilon < M$, the set $S := ((\epsilon, 1 - \epsilon) \cup (1 + \epsilon, M)) \cap \mathbb{Q}$ is not a set of topological multiplicative recurrence. In other words, if S does not have $0, 1$ or ∞ as an accumulation point, then S is not a set of topological multiplicative recurrence.*

Proof. Let ϵ and M be as in the hypothesis of the lemma. Choose $c_1, c_2, a \in \mathbb{R}$ such that

$$c_1 < 1 - \epsilon < 1 + \epsilon < c_2$$

and

$$a > \max\{c_2/\epsilon, M/c_1\}.$$

Then it follows that

$$\bigcup_{k \in \mathbb{Z}} (c_1 a^k, c_2 a^k) \subset (0, \epsilon) \cup (1 - \epsilon, 1 + \epsilon) \cup (M, \infty).$$

Let $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ and consider topological $(\mathbb{Q}^{>0}, \times)$ -system (S^1, T) defined as $T_q(e(x)) = e(\log_a q)e(x)$ for every $q \in \mathbb{Q}^{>0}$ and $x \in [0, 1)$ (here $e(x) := e^{2\pi i x}$). Let $\epsilon_1 = -\log_a c_1, \epsilon_2 = \log_a c_2$ and let $B = \{e(x) : x \in (1 - \epsilon_1, 1 + \epsilon_2)\}$ be a neighborhood of $e(0)$ in S^1 . We have $T_q e(0) \in B$ if and only if $\log_a q \in \bigcup_{k \in \mathbb{Z}} (k - \epsilon_1, k + \epsilon_2)$, or equivalently $q \in \bigcup_{k \in \mathbb{Z}} (a^{-\epsilon_1} a^k, a^{\epsilon_2} a^k)$. It follows that

$$\{q \in \mathbb{Q}^{>0} : T_q e(0) \in B\} \subset \bigcup_{k \in \mathbb{Z}} (a^{-\epsilon_1} a^k, a^{\epsilon_2} a^k) \subset (0, \epsilon) \cup (1 - \epsilon, 1 + \epsilon) \cup (M, \infty).$$

Since every set of topological multiplicative recurrence must intersect $\{q \in \mathbb{Q}^{>0} : T_q e(0) \in B\}$ we conclude that R must intersect $(0, \epsilon) \cup (1 - \epsilon, 1 + \epsilon) \cup (M, \infty)$. Therefore the set S defined in Lemma 3.1 is not a set of topological multiplicative recurrence. \square

We now prove parts (1) and (2) of Theorem 1.6.

Proposition 3.2 (Part (1) of Theorem 1.6). *Let $a, c, \ell \in \mathbb{N}$, $b, d \in \mathbb{Z}$ with $a \neq c$. Then $S = \{(an + b)^\ell / (cn + d)^\ell : n \in \mathbb{N}\}$ is not a set of topological multiplicative recurrence.*

Proof. First note that $(an + b)^\ell / (cn + d)^\ell \rightarrow (a/c)^\ell$ as $n \rightarrow \infty$. Therefore, for any $\epsilon > 0$, the set $S \setminus ((a/c)^\ell - \epsilon, (a/c)^\ell + \epsilon)$ is finite. Moreover, since $a \neq c$, for sufficiently small ϵ , we have $((a/c)^\ell - \epsilon, (a/c)^\ell + \epsilon)$ does not contain $0, 1$. Hence, S does not have $0, 1$ or ∞ as an accumulation point, and by Lemma 3.1, the set S is not a set of topological multiplicative recurrence. \square

Proposition 3.3 (Part (2) of Theorem 1.6). *Let $a, \ell \in \mathbb{N}$ and $b, d \in \mathbb{Z}$. Suppose that $b \neq d$ and there exists a prime p for which $p|a$ but $p \nmid bd$. Then $S = \{(an + b)^\ell / (an + d)^\ell : n \in \mathbb{N}\}$ is not a set of topological multiplicative recurrence.*

Proof. Since S is a subset of $S' = \{(pn + b)^\ell / (pn + d)^\ell : n \in \mathbb{N}\}$, it suffices to prove that S' is not a set of topological multiplicative recurrence. In view of Corollary 2.14, we need to prove that $S'' = \{(pn + b) / (pn + d) : n \in \mathbb{N}\}$ is not a set of topological multiplicative recurrence.

Because $b \neq d$, there exists $u \in \mathbb{N}$ such that p^u does not divide $b - d$. Let χ be the finite coloring of \mathbb{N} defined recursively as

$$\chi(n) = \begin{cases} n \bmod p^u & \text{if } p \nmid n \\ \chi(n/p) & \text{if } p|n. \end{cases}$$

We shall show that S'' is not a set of recurrence for the coloring χ . By contradiction, assume there exist monochromatic $x, y \in \mathbb{N}$ such that

$$(2) \quad \frac{x}{y} = \frac{pn + b}{pn + d}.$$

Write $x = p^{k_x} x_0$ and $y = p^{k_y} y_0$ where $k_x, k_y \in \mathbb{N} \cup \{0\}$ and $p \nmid x_0 y_0$. By the definition of the coloring χ , we have that $x_0 \equiv y_0 \pmod{p^u}$.

From (2), we have $x(pn + d) = y(pn + b)$. It follows that $p^{k_x} x_0 (pn + d) = p^{k_y} y_0 (pn + b)$. Since $pn + b$ and $pn + d$ are coprime to p , we deduce that $k_x = k_y$ and $x_0 (pn + d) = y_0 (pn + b)$. As $x_0 \equiv y_0 \pmod{p^u}$, it must be that $pn + d \equiv pn + b \pmod{p^u}$, or equivalently, $b \equiv d \pmod{p^u}$. This contradicts our assumption that p^u does not divide $b - d$ and our proof finishes. \square

For the proof of part (3) of Theorem 1.6, we need a recurrence result in topological dynamical systems:

Lemma 3.4. *Let (X, T) be a topological $(\mathbb{N}, +)$ -system where X is a compact metric space with the metric d . Suppose that there exists $x \in X$ such that $\{T^n x : n \in \mathbb{N}\}$ is dense in X . Then for every $y \in X, \epsilon > 0$ and $N \in \mathbb{N}$, there exists $m_0 \in \mathbb{N}$ such that $d(T^{i+m_0} x, T^i y) < \epsilon$ for all $i \in [N]$.*

Proof. For $i \in [N]$, the map $T^i : X \rightarrow X$ is continuous, hence uniformly continuous. Thus, there exists $\delta > 0$ such that for $w, z \in X$, $d(w, z) < \delta$ implies $d(T^i w, T^i z) < \epsilon$ for all

$i \in [N]$. Since $\{T^n x : n \in \mathbb{N}\}$ is dense in X , for any $y \in Y$ we can find $m_0 \in \mathbb{N}$ such that $d(T^{m_0} x, y) < \delta$. Then the choice of δ implies that $d(T^{i+m_0} x, T^i y) < \epsilon$ for all $i \in [N]$. \square

Next we prove the following special case of part (3) of Theorem 1.6.

Lemma 3.5. *For any $a \in \mathbb{N}$, the sets $\{(an+1)/(an) : n \in \mathbb{N}\}$ and $\{(an-1)/(an) : n \in \mathbb{N}\}$ are sets of topological multiplicative recurrence.*

Proof. We only prove the first set is a set of topological multiplicative recurrence as the proof for the second set is the same. Fix $r \in \mathbb{N}$ with $r \geq 1$. Let \mathbb{N}_0 denote $\mathbb{N} \cup \{0\}$ and let $X_0 = [r]^{\mathbb{N}_0} = \{(w(n))_{n \in \mathbb{N}_0} : w(n) \in [r]\}$. Define a metric d on X_0 as the following: For $w = (w(n))_{n \in \mathbb{N}_0}$ and $z = (z(n))_{n \in \mathbb{N}_0}$,

$$d(w, z) := \sum_{n \in \mathbb{N}_0} \frac{|w(n) - z(n)|}{2^n}.$$

Under this metric, X_0 becomes a compact metric space and $d(w, z) < 1$ implies $w(0) = z(0)$. Let $T : X_0 \rightarrow X_0$ be the left shift which is defined as $T(w(n))_{n \in \mathbb{N}_0} = (w(n+1))_{n \in \mathbb{N}_0}$. Then T is a continuous map.

Let $c : \mathbb{N} \rightarrow [r]$ be a finite coloring of \mathbb{N} . We need to find $x, y \in \mathbb{N}$ of the same color and $n \in \mathbb{N}$ such that $y/x = (an+1)/an$. This is equivalent to finding $\{x, x+k\}$ of the same color with $ak|x$ (indeed, writing $x = nak$ and $y = x+k$ we have $y/x = (an+1)/an$). By regarding c as an element of X_0 , we define X to be the closure of $\{T^n c : n \in \mathbb{N}_0\}$ in X_0 . It follows that (X, T) is a topological $(\mathbb{N}_0, +)$ -system. Let (Y, T) be a minimal subsystem of (X, T) .² For each color $j \in [r]$, let U_j be the cylinder $U_j = \{x \in X_0 : x(0) = j\}$. By minimality, the return times of points in $Y \cap U_j$ back to $Y \cap U_j$ are uniformly bounded, i.e. there exists $N_j \in \mathbb{N}$ such that for all $y \in Y \cap U_j$, there exists $n = n(y) \in [N_j]$ satisfying $T^n y \in U_j \cap Y$ (for example, see [1, Chapter 1]). Setting $N_0 = \max\{N_j : j \in [r]\}$, we have that for all $y \in Y$ and $n \in \mathbb{N}$, there exists $1 \leq n' \leq N_0$ for which $y(n) = y(n+n')$.

Fix $y_0 \in Y$. By Lemma 3.4, there exists $m_0 \in \mathbb{N}$ such that $d(T^{i+m_0} c, T^i y_0) < 1$ for all $i \in [aN_0!]$ (the number $aN_0!$ is chosen here because later we will use the fact that $an' | aN_0!$ for all $1 \leq n' \leq N_0$). In particular, we have $c(m_0+i) = y_0(i)$ for $1 \leq i \leq aN_0!$. Let $i_0 \in [aN_0!]$ satisfy $m_0 + i_0 \equiv 0 \pmod{aN_0!}$. From previous paragraph, there exists $1 \leq n' \leq N_0$ such that $y_0(i_0) = y_0(i_0+n')$. Hence it follows that $c(m_0+i_0) = c(m_0+i_0+n')$. By writing $x = m_0+i_0$ and $k = n'$, we have $c(x) = c(x+k)$ with $ak|x$, finishing our proof. \square

We are now ready to prove part (3) of Theorem 1.6.

²The existence of minimal subsystems follows from an application of Zorn's lemma (cf. [1, Theorem 1.4]).

Proposition 3.6 (Part (3) of Theorem 1.6). *For $a, b, d, \ell \in \mathbb{Z}$ with $a, \ell > 0$ and $a|b$ or $a|d$,*

$$S = \left\{ \left(\frac{an + b}{an + d} \right)^\ell : n \in \mathbb{N} \right\}$$

is a set of topological multiplicative recurrence.

Proof. In view of Corollary 2.14, it suffices to show that

$$S' = \left\{ \frac{an + b}{an + d} : n \in \mathbb{N} \right\}$$

is a set of topological multiplicative recurrence. Without loss of generality, assume $a|d$ and $d = ad_1$. If $b = d$, then $S' = \{1\}$ which is trivially a set of multiplicative recurrence. If $b > d$, then we have

$$S' = \left\{ \frac{a(n + d_1) + b - ad_1}{a(n + d_1)} : n \in \mathbb{N} \right\}$$

which contains the set

$$\left\{ \frac{a(n + d_1) + b - ad_1}{a(n + d_1)} : n + d_1 \equiv 0 \pmod{b - ad_1} \right\} = \left\{ \frac{am + 1}{am} : m \in \mathbb{N} \right\}.$$

By Lemma 3.5, the last set is a set of topological multiplicative recurrence, and hence so is S' .

On the other hand, if $b < d$, then S' contains the set

$$\left\{ \frac{a(n + d_1) + b - ad_1}{a(n + d_1)} : n + d_1 \equiv 0 \pmod{ad_1 - b} \right\} = \left\{ \frac{am - 1}{am} : m \in \mathbb{N} \right\}$$

which is again a set of topological multiplicative recurrence. \square

Next we prove Corollary 1.7.

Proof of Corollary 1.7. Let $f : \mathbb{N} \rightarrow \mathbb{C}$ be a completely multiplicative function with $|f(n)| = 1$ for $n \in \mathbb{N}$ and let $a, k \in \mathbb{N}$. We need to prove that,

$$\liminf_{n \rightarrow \infty} |f(an + k) - f(an)| = 0.$$

Let $\epsilon > 0$. Consider the topological (\mathbb{N}, \times) -system (S^1, T) where $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ and $T_n e^{2\pi i x} = f(n) e^{2\pi i x}$ for all $x \in [0, 1)$ and $n \in \mathbb{N}$. Let $A = \{e^{2\pi i x} : x \in (-\epsilon/2, \epsilon/2)\} \subset S^1$. Then by Proposition 3.6 and Proposition 2.13, there exist infinitely many $n \in \mathbb{N}$ such that $T_{(an+k)m} A \cap T_{anm} A \neq \emptyset$ for some $m \in \mathbb{N}$ (which may depend on n). This implies $f((an+k)m) A \cap f(anm) A \neq \emptyset$, or equivalently, $f(m) f(an+k) A \cap f(m) f(an) A \neq \emptyset$. Since multiplication by $f(m)$ is an isometry, we have

$$f(an+k) A \cap f(an) A \neq \emptyset.$$

It follows that $|f(an+k) - f(an)| \leq \epsilon$ for infinitely many n . Since ϵ is arbitrary, we have $\liminf_{n \rightarrow \infty} |f(an+k) - f(an)| = 0$. \square

Remark 3.7. Theorem 1.6 implies that for any finite coloring of \mathbb{N} and every $k \in \mathbb{N}$, there exist $a, n \in \mathbb{N}$ such that $an|x$ and the set

$$\left\{ x, x \frac{an+k}{an} \right\}$$

is monochromatic. It is natural to ask if, more generally, we can find $a, n \in \mathbb{N}$ for which $an|x$ and the set

$$\left\{ x, x \frac{an+1}{an}, x \frac{an+2}{an}, \dots, x \frac{an+k}{an} \right\}$$

is monochromatic. It turns out that the answer is negative, even in the case $a = 1$ and $k = 2$, as shown by the following example.

Let $c : \mathbb{N} \rightarrow \{1, 2\}$ be the 3-Rado coloring: For $m \in \mathbb{N}$, write $m = 3^k q$ where $k \in \mathbb{N} \cup \{0\}$ and $3 \nmid q$. Then color $c(m) = 1$ if $q \equiv 1 \pmod{3}$ and $c(m) = 2$ if $q \equiv 2 \pmod{3}$. Note that in every 3 consecutive integers, there is a number congruent to 1 mod 3 and another congruent to 2 mod 3, therefore there are no 3 consecutive numbers with the same color. On the other hand, observe that $c(x) = c(y)$ if and only if $c(xz) = c(yz)$. Indeed, this is obvious if z is a power of 3; and if z is co-prime to 3 then $c(xz) \equiv c(x)z \pmod{3}$. If the set

$$\left\{ \frac{x}{n}, \frac{x}{n}(n+1), \frac{x}{n}(n+2) \right\}$$

were monochromatic for some $x, n \in \mathbb{N}$ with $n|x$, so would be the set $\{n, n+1, n+2\}$, a contradiction.

3.2. Linear polynomials. Let (X, T) be an (\mathbb{N}, \times) -system. If X is a finite set, we say that $(X, (T_n)_{n \in \mathbb{N}})$ is a *finite* (\mathbb{N}, \times) -system. The following theorem classifies which sets of the form $a\mathbb{N} + b$ that are sets of multiplicative recurrence, and hence implies Theorem 1.10.

Theorem 3.8. *Let $a, b \in \mathbb{N}$ and $S = \{an + b : n \in \mathbb{N}\}$. The followings are equivalent:*

- (i) $a|b(b-1)$.
- (ii) S is a multiplicative semigroup.
- (iii) S contains an infinite multiplicative semigroup.
- (iv) S is a set of measurable recurrence for (\mathbb{N}, \times) -systems.
- (v) S is a set of topological recurrence for finite (\mathbb{N}, \times) -systems.

Proof. (i) \Rightarrow (ii): If $a|b(b-1)$, then for any $ax + b, ay + b \in S$, we have

$$(ax + b)(ay + b) = a \left(axy + bx + by + \frac{b(b-1)}{a} \right) + b \in S.$$

(ii) \Rightarrow (iii): Obvious.

(iii) \Rightarrow (iv): This follows from the Poincaré Recurrence Theorem.

(iv) \Rightarrow (v): Obvious.

(v) \Rightarrow (i): We prove the contrapositive. Let a, b be such that $a \nmid b(b-1)$. It suffices to construct a finite (\mathbb{N}, \times) -system $(X, (T_n)_{n \in \mathbb{N}})$ such that whenever $n \in S$, the permutation T_n fixes no element. Let $a' = a/(a, b)$. Observe that $b \not\equiv 1 \pmod{a'}$, for otherwise $b(b-1)$ would be a multiple of $a = (a, b)a'$. We need to consider separate cases:

Case 1: $(a', b) = 1$. In this case every $n \in S$ satisfies $(n, a') = 1$ and $n \equiv b \not\equiv 1 \pmod{a'}$. Let $X = \{x \in \{0, 1, \dots, a' - 1\} : (x, a') = 1\}$. For $n \in \mathbb{N}$, let $T_n: X \rightarrow X$ be defined as follows. Let A be the set of all $q \in \mathbb{N}$ such that the all prime divisors of q also divide a' . Any natural number n can be written uniquely as $n = uv = u(n)v(n)$ where $u \in A, v \in \mathbb{N}$ and $(v, a') = 1$. For $x \in X$, define $T_n x = xv(n) \pmod{a'}$. Notice that $v(nm) = v(n)v(m)$, so $(T_n)_{n \in \mathbb{N}}$ is indeed an action of (\mathbb{N}, \times) on X . Since every $n \in S$ satisfies $(n, a') = 1$ and $n \not\equiv 1 \pmod{a'}$, $v(n) = n \not\equiv 1 \pmod{a'}$. Therefore, for $n \in S$, we have T_n does not fix any point in X .

Case 2: $(a', b) > 1$. Let p be a prime which divides (a', b) and let $k \in \mathbb{N}$ be such that $p^{k-1} | b$ but $p^k \nmid b$. Let $X = \mathbb{Z}_k$ and let $T_n: X \rightarrow X, n \in \mathbb{N}$ be defined as follows. For $n \in \mathbb{N}$, let $u(n)$ and $v(n)$ be the unique non-negative integers satisfying $n = p^{u(n)}v(n)$ and $p \nmid v(n)$. For $x \in X$, define $T_n x := x + u(n) \pmod{k}$. Since $u(nm) = u(n) + u(m)$, $(T_n)_{n \in \mathbb{N}}$ indeed defines an action of (\mathbb{N}, \times) on X . Because $(a', b/(a, b)) = 1$ and $p | a'$, it follows that $p \nmid b/(a, b)$. On the other hand, $p^{k-1} | b$. Therefore, $p^{k-1} | (a, b)$, and hence $p^k | a = (a, b)a'$. Thus for any $n \in S$, we have $u(n) = k - 1$, which implies that $T_n x = x - 1 \pmod{k}$ for every $x \in X$. In particular, T_n does not fix any element of X . \square

A polynomial $P \in \mathbb{Z}[x]$ is called *divisible* if for any $q \in \mathbb{N}$, there exists $n \in \mathbb{N}$ such that $q | P(n)$. As proven in [16], the set $\{P(n) : n \in \mathbb{N}\}$ is a set of additive topological (and measurable) recurrence if and only if P is divisible.

Corollary 3.9. *Let $P \in \mathbb{Z}[x]$. If $S = \{P(n) : n \in \mathbb{N}\}$ is a set of topological multiplicative recurrence, then $R = \{P(n)(P(n) - 1) : n \in \mathbb{N}\}$ is a set of measurable additive recurrence, i.e. the polynomial $P(P - 1)$ is divisible.*

Proof. Assume $P(P - 1)$ is not divisible. Then there exists $a \in \mathbb{N}$ such that $a \nmid P(n)(P(n) - 1)$ for all $n \in \mathbb{N}$. Hence a

$$(3) \quad \{P(n) : n \in \mathbb{N}\} \subset \bigcup_{\substack{0 \leq b \leq a-1 \\ a \nmid b(b-1)}} a\mathbb{N} + b.$$

In view of Theorem 3.8, for each $b \in \{0, \dots, a - 1\}$ such that $a \nmid b(b - 1)$, the set $a\mathbb{N} + b$ is not a set of multiplicative recurrence. Invoking [7, Theorem 2.7 (b)] it follows that the union in the right hand side of (3) can not be a set of recurrence. \square

Example 3.10. As an application of Corollary 3.9, the set $\{n^2 + 3 : n \in \mathbb{N}\}$ is not a set of topological multiplicative recurrence. This is because the polynomial $Q(n) = n^4 + 5n^2 + 6$ is not divisible, as $5 \nmid Q(n)$ for any $n \in \mathbb{N}$.

Any polynomial $P \in \mathbb{Z}[x]$ with $P(0) = 0$ is divisible, so in that case the set $S = \{P(n) : n \in \mathbb{N}\}$ is a set of measurable additive recurrence. However, this set is not a set of multiplicative recurrence in general as the following example shows:

Example 3.11. Let p be a prime. The set $S = \{pn^2 : n \in \mathbb{N}\}$ is not a set of topological multiplicative recurrence. Indeed, let $E = \{p^{2k}\ell : k \in \mathbb{N} \cup \{0\}, \ell \in \mathbb{N}, p \nmid \ell\}$ and $F = \{p^{2k+1}\ell : k \in \mathbb{N} \cup \{0\}, \ell \in \mathbb{N}, p \nmid \ell\}$. Then $E \cup F = \mathbb{N}$. For every $x, y \in E$ or $x, y \in F$, x/y has the form $p^{2k}\ell_1/\ell_2$ for some $k \in \mathbb{Z}$ and $\ell_1, \ell_2 \in \mathbb{N}$ with $p \nmid \ell_1\ell_2$. It follows that $x/y \notin S$, hence S is not a set of multiplicative recurrence.

Example 3.11 can also be used to show that the converse to Corollary 3.9 is false in general. Indeed, take $P(n) = pn^2$. Then $P(n)(P(n)-1) = pn^2(pn^2-1)$ is divisible, but $\{P(n) : n \in \mathbb{N}\}$ is not set of topological multiplicative recurrence.

4. ALGEBRAIC SETS THAT CONTAIN MULTIPLICATIVE SEMIGROUPS

As mentioned in Section 2, every subsemigroup of (\mathbb{N}, \times) is a set of multiplicative recurrence. With the ultimate goal of understanding which algebraically defined sets are sets of multiplicative recurrence, it is natural to also study sets which are (or contain) a semigroup. In this section we investigate this question for sets that are the image of a polynomial or the image of a rational function.

4.1. Polynomial sets that contain multiplicative semigroups. In this section we prove Theorem 1.9. We first need some lemmas.

Lemma 4.1. *Let $d \geq 2$ and $P(x) = a_dx^d + a_{d-2}x^{d-2} + \dots + a_1x + a_0 \in \mathbb{Q}[x]$ such that at least one of a_0, a_1, \dots, a_{d-2} is non-zero and $a_d > 0$. Then $S = \{P(n) : n \in \mathbb{N}\}$ does not contain any infinite subsemigroup of $(\mathbb{Q}^{>0}, \times)$.*

Proof. First we show that, for any $D \in \mathbb{N} \setminus \{1\}$, there are only finitely many $n \in \mathbb{N}$ such that $D^d P(n) = P(Dn)$. Indeed, otherwise, the polynomial $D^d P(x) - P(Dx)$ would have infinitely many roots, and hence $D^d P(x) = P(Dx)$ for all $x \in \mathbb{R}$. It would follow that $P(D^k) = P(1)(D^k)^d$ for all $k \in \mathbb{N}$. This implies that the equation $P(x) = P(1)x^d$ has infinitely many solutions. So $P(x) = P(1)x^d$ for all $x \in \mathbb{R}$. This contradicts our assumption that at least one of a_0, a_1, \dots, a_{d-2} is nonzero.

Next we assume, for the sake of a contradiction, that there exists $D \in \mathbb{N} \setminus \{1\}$ such that $\{D^n : n \in \mathbb{N}\} \subset S$. Then there exist infinitely many $m > n \in \mathbb{N}$ such that

$$(4) \quad D^d P(n) = P(m).$$

Using the first paragraph of the proof, there are infinitely many solutions to (4) with $m \neq Dn$. Next, observe that (4) can be written as

$$(5) \quad a_d(m^d - (Dn)^d) = \sum_{j=0}^{d-2} a_j(D^d n^j - m^j).$$

Note that for all $x, y \in \mathbb{N}$ with $x \neq y$, $|x^d - y^d| > (\max\{x, y\})^{d-1}$. Hence if $m \neq Dn$ for some $m, n \in \mathbb{N}$, then $|m^d - (Dn)^d| > (\max\{m, Dn\})^{d-1}$. On the other hand,

$$\left| \sum_{j=0}^{d-2} a_j(D^d n^j - m^j) \right| \leq 2(d-1) \max_{0 \leq j \leq d-2} \{|a_j|\} (\max\{m, Dn\})^{d-2}.$$

Therefore, from (5) we derive that

$$a_d \max\{m, Dn\}^{d-1} < 2(d-1) \max_{0 \leq j \leq d-2} \{|a_j|\} \max\{m, Dn\}^{d-2}$$

for infinitely many $m, n \in \mathbb{N}$. This is impossible and hence it yields the desired contradiction. \square

Lemma 4.2. *Let $P \in \mathbb{Z}[x]$. Then there exist $a, b \in \mathbb{Z}$ and $Q \in \mathbb{Q}[x]$ such that $P(x) = Q(ax+b)$ and writing $Q(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$ we have $a_{d-1} = 0$. If the leading coefficient of P is positive, then $a > 0$.*

Proof. Let $P(x) = b_d x^d + \dots + b_0$ and factor it over \mathbb{C} as $b_d \prod_{i=1}^d (x - \alpha_i)$, where $\alpha_1, \dots, \alpha_d \in \mathbb{C}$ are the roots of P counted with multiplicity. It follows that $\sum_{i=1}^d \alpha_i = -b_{d-1}/b_d$. Let $a = db_d$, $b = b_{d-1}$ and define $Q(y) := P((y-b)/a)$. Observe that $Q(y) = 0$ if and only if $y = a\alpha_i + b$ for some $1 \leq i \leq d$. Therefore the sum of the roots of Q is 0, which implies that $a_{d-1} = 0$. \square

We are ready to prove Theorem 1.9. In fact we prove the following more general result.

Theorem 4.3. *Let $P \in \mathbb{Z}[x]$ and $S = \{P(n) : n \in \mathbb{N}\}$. The following are equivalent:*

- (i) S is an infinite subsemigroup of $(\mathbb{Q}^{>0}, \times)$.
- (ii) S contains an infinite subsemigroup of $(\mathbb{Q}^{>0}, \times)$.
- (iii) $P(x) = (ax+b)^d$ for some $a, d \in \mathbb{N}$, $b \in \mathbb{Z}$ with $a|b(b-1)$.

Proof. (iii) \Rightarrow (i): Assume $Q(x) = (ax+b)^d$ with $a|b(b-1)$. Then for any $x, y \in \mathbb{N}$,

$$Q(x)Q(y) = (ax+b)^d (ay+b)^d = \left(a \left(axy + bx + by + \frac{b(b-1)}{a} \right) + b \right)^d \in S.$$

Hence S is a multiplicative semigroup.

(i) \Rightarrow (ii): Trivial.

(ii) \Rightarrow (iii): Assume that $S = \{P(n) : n \in \mathbb{N}\}$ contains an infinite multiplicative semigroup of $\mathbb{Q}^{>0}$. Then the leading coefficient of P is positive. Write $P(x) = Q(ax+b)$ as in Lemma 4.2, noting that $a > 0$. Then we have $\{P(n) : n \in \mathbb{N}\} = \{Q(an+b) : n \in \mathbb{N}\} \subset \{Q(n) : n \in \mathbb{N}\}$. It then follows that $\{Q(n) : n \in \mathbb{N}\}$ contains a semigroup. By Lemma 4.1, $Q(x) = a_d x^d$ for some $d \in \mathbb{N}$ and $a_d \in \mathbb{Q}$. Since $\{Q(n) : n \in \mathbb{N}\}$ contains a semigroup, there exist $x, y, z \in \mathbb{N}$ such that $Q(x)Q(y) = Q(z)$. In other words, $a_d^2(xy)^d = a_d z^d$, or $a_d = (z/(xy))^d$. Let $c = z/(xy) \in \mathbb{Q}^{>0}$, we get $a_d = c^d$. Hence $P(x) = (c(ax+b))^d = (cax+cb)^d$.

By abuse of notation, assume that $P(x) = (ax+b)^d$ for some $a, b \in \mathbb{Q}$. Since $P \in \mathbb{Z}[x]$, we have $a, b \in \mathbb{Z}$. Because S contains an infinite multiplicative semigroup, there exists $D \in \mathbb{N} \setminus \{1\}$ such that for all $k \in \mathbb{N}$, there exists $x \in \mathbb{N}$ and $(ax+b)^d = D^{kd}$. In other words, $ax+b = D^k$. It follows that $D^k \equiv b \pmod{a}$ for all $k \in \mathbb{N}$. Hence we have simultaneously that $D^{2k} \equiv b^2$ and $D^{2k} \equiv b \pmod{a}$. This implies that $b^2 \equiv b \pmod{a}$, or $a|b(b-1)$, which finishes the proof. \square

4.2. Rational functions that do not contain a semigroup. We prove Proposition 1.11 in this section. In addition, we show that many other rational functions of interest do not contain infinite multiplicative semigroups.

Lemma 4.4. *Let $\ell \geq 2$, $q_1, q_2, \dots, q_\ell \in \mathbb{R} \setminus \{0\}$ be non-zero and $|q_i| \neq |q_j|$ for all $i \neq j$. Let $a_1, \dots, a_\ell \in \mathbb{R}$ be such that $a_1 q_1^k + \dots + a_\ell q_\ell^k = 0$ for infinitely many $k \in \mathbb{N}$. Then $a_1 = a_2 = \dots = a_\ell = 0$.*

Proof. By contradiction, assume some a_i are non-zero. By discarding those a_i that are zero, without loss of generality, we may assume that none of the a_i are zero.

Assume $|q_1| = \max\{|q_i| : 1 \leq i \leq \ell\} > 0$. Then we have

$$|a_1 q_1^k| = |a_2 q_2^k + \dots + a_\ell q_\ell^k|.$$

It follows that

$$|a_1| = |a_2 (q_2/q_1)^k + \dots + a_\ell (q_\ell/q_1)^k|$$

for infinitely many $k \in \mathbb{N}$. But this is impossible since the right hand side approaches zero as $k \rightarrow \infty$. \square

We are ready to prove Proposition 1.11.

Proof of Proposition 1.11. We only give a proof that the set $S = \{(m^2 + n^2)/(2mn) : m, n \in \mathbb{N}\}$ does not contain an infinite subsemigroup of $(\mathbb{Q}^{>0}, \times)$ as the proof for the other set is the same. By contradiction, assume that there exist $p, q \in \mathbb{Z}, p \neq q, (p, q) = 1$ such that $\{(p/q)^k : k \in \mathbb{N}\} \subset S$. By replacing (p/q) by $(p/q)^2$, we can assume $p, q > 0$. Then it follows

that for every $k \in \mathbb{N}$, there exist $m, n \in \mathbb{N}$ such that

$$(6) \quad \frac{p^k}{q^k} = \frac{m^2 + n^2}{2mn}.$$

We can dividing both m and n by $\gcd(m, n)$ and (6) still holds. Therefore, without loss of generality, we may assume $(m, n) = 1$. Then

$$2p^k mn = q^k(m^2 + n^2).$$

Since $(p, q) = 1$, it follows that $q^k | 2mn$. On the other hand, since $(m, n) = 1$, $(mn, m^2 + n^2) = 1$. Thus $mn | q^k$. It follows that $q^k = mn$ or $q^k = 2mn$.

If $q^k = mn$, then $2p^k = m^2 + n^2$. Since $(m, n) = 1$, $m = q_1^k$ and $n = q_2^k$ for some $q_1 q_2 = q$. Hence

$$(7) \quad 2p^k = (q_1^2)^k + (q_2^2)^k.$$

If $q^k = 2mn$, then $p^k = m^2 + n^2$. Similarly to above, $m = (q_1)^k/2$ and $n = q_2^k$ for some $q_1 q_2 = q$. We then have $p^k = q_1^{2k}/4 + q_2^{2k}$, or equivalently,

$$(8) \quad 4p^k = (q_1^2)^k + 4(q_2^2)^k.$$

Since the set $\{(q_1, q_2) \in \mathbb{N}^2 : q_1 q_2 = q\}$ is finite, there must be some fixed q_1, q_2 such that either (7) or (8) is true for infinitely many $k \in \mathbb{N}$. But, in view of Lemma 4.4, this is impossible, and hence we obtained the desired contradiction. \square

Let $\ell_1, \ell_2, \ell_3, \ell_4 \in \mathbb{Z}$ be pairwise distinct and let

$$(9) \quad S = \left\{ \frac{(m + \ell_1 n)(m + \ell_2 n)}{(m + \ell_3 n)(m + \ell_4 n)} : m, n \in \mathbb{N} \right\}.$$

It is shown in [11] that the set S in (9) is a set of measurable multiplicative recurrence. In the following proposition, we show that S does not contain any infinite subsemigroup of $(\mathbb{Q}^{>0}, \times)$.

Proposition 4.5. *Let $\ell_1, \ell_2, \ell_3, \ell_4 \in \mathbb{Z}$ be pairwise distinct. Then the set*

$$S = \left\{ \frac{(m + \ell_1 n)(m + \ell_2 n)}{(m + \ell_3 n)(m + \ell_4 n)} : m, n \in \mathbb{N} \right\}$$

does not contain any infinite subsemigroup of $(\mathbb{Q}^{>0}, \times)$.

Proof. By contradiction, assume there exist $p \in \mathbb{Z}, q \in \mathbb{N}$ with $(p, q) = 1$ such that for all $k \in \mathbb{N}$, there exist $m, n \in \mathbb{N}$ such that

$$\frac{(m + \ell_1 n)(m + \ell_2 n)}{(m + \ell_3 n)(m + \ell_4 n)} = \frac{p^k}{q^k}.$$

Dividing m, n by $\gcd(m, n)$, we can assume $(m, n) = 1$. We then have

$$q^k(m + \ell_1 n)(m + \ell_2 n) = p^k(m + \ell_3 n)(m + \ell_4 n).$$

It follows that $q^k | p^k(m + \ell_3n)(m + \ell_4n)$. But since $(p, q) = 1$, it implies that $q^k | (m + \ell_3n)(m + \ell_4n)$. Similarly, $p^k | (m + \ell_1n)(m + \ell_2n)$. Let

$$t = \frac{(m + \ell_1n)(m + \ell_2n)}{p^k} = \frac{(m + \ell_3n)(m + \ell_4n)}{q^k} \in \mathbb{Z}.$$

Therefore $t | \gcd((m + \ell_1n)(m + \ell_2n), (m + \ell_3n)(m + \ell_4n))$.

For $i, j \in \{1, 2, 3, 4\}$, let $d = \gcd(m + \ell_in, m + \ell_jn)$. Then $d | (\ell_j - \ell_i)n$ and $d | ((\ell_j - \ell_i)m + (\ell_j - \ell_i)\ell_in)$. Therefore, $d | (\ell_j - \ell_i)m$. Since $(m, n) = 1$, it follows that $d | (\ell_j - \ell_i)$. We deduce that $t | (\ell_3 - \ell_1)(\ell_3 - \ell_2)(\ell_4 - \ell_1)(\ell_4 - \ell_2)$. We then have

$$(m + \ell_1n)(m + \ell_2n) = tp^k$$

and

$$(m + \ell_3n)(m + \ell_4n) = tq^k.$$

Since $(m + \ell_1n, m + \ell_2n) | (\ell_2 - \ell_1)$, we deduce that there exists some $k_0 = k_0(\ell_1, \ell_2, \ell_3, \ell_4)$ such that

$$(10) \quad m + \ell_1n = u_1p_1^{k-k_0} \text{ and } m + \ell_2n = u_2p_2^{k-k_0}$$

where $(p_1, p_2) = 1$, $p_1p_2 = p$ and $u_1u_2 = tp^{k_0}$. Similarly, there exists $k_1 = k_1(\ell_1, \ell_2, \ell_3, \ell_4)$ such that

$$(11) \quad m + \ell_3n = v_1q_1^{k-k_1} \text{ and } m + \ell_4n = v_2q_2^{k-k_1}$$

where $(q_1, q_2) = 1$, $q_1q_2 = q$ and $v_1v_2 = tq^{k_1}$.

Since there are only finitely many choices of t, u_i, v_i, p_i, q_i for $i = 1, 2$, it follows that there exist fixed u_i, v_i, p_i, q_i for $i = 1, 2$ for which there are infinitely many $k \in \mathbb{N}$ such that (10) and (11) simultaneously have solutions $(m, n) \in \mathbb{N}^2$. Solving these equations, we get

$$n = \frac{u_2p_2^{k-k_0} - u_1p_1^{k-k_0}}{\ell_2 - \ell_1} = \frac{v_2q_2^{k-k_1} - v_1q_1^{k-k_1}}{\ell_3 - \ell_4}.$$

In particular,

$$\frac{u_2}{(\ell_2 - \ell_1)p_2^{k_0}} \times p_2^k - \frac{u_1}{(\ell_2 - \ell_1)p_1^{k_0}} \times p_1^k - \frac{v_2}{(\ell_3 - \ell_4)q_2^{k_1}} \times q_2^k + \frac{v_1}{(\ell_3 - \ell_4)q_1^{k_1}} \times q_1^k = 0$$

for infinitely many $k \in \mathbb{N}$. Since p_1, p_2, q_1, q_2 are pairwise coprime, we can apply Lemma 4.4 to show that $u_i = v_i = 0$ for $i = 1, 2$. It follows from (10) that $m = n = 0$. This contradicts our assumption that $m, n \in \mathbb{N}$ finishing the proof. \square

5. ADDITIVE AVERAGES OF MULTIPLICATIVE RECURRENCE SEQUENCES

5.1. Multiplicative subsemigroups of \mathbb{N} . Recall from Section 2 that a subset $S \subset G$ is syndetic if there exists a finite set $F \subset G$ such that $\bigcup_{x \in F} S/x = G$. As Proposition 2.2 shows, every syndetic set $F \subset G$ has positive density with respect to any Følner sequence in G . The next result shows that in the case when (G, \times) is a subsemigroup of (\mathbb{N}, \times) , then a (multiplicative) syndetic subset of G has positive “upper density” also with respect to the “additive” sequence $(G \cap [N])_{N \in \mathbb{N}}$.

Lemma 5.1. *Let (G, \times) be a subsemigroup of (\mathbb{N}, \times) and S be a syndetic subset of G . Then*

$$\limsup_{N \rightarrow \infty} \mathbb{E}_{n \in G \cap [N]} 1_S(n) > 0.$$

Moreover, if G has positive lower additive density in \mathbb{N} , then

$$\liminf_{N \rightarrow \infty} \mathbb{E}_{n \in G \cap [N]} 1_S(n) > 0.$$

Proof. We first claim that for any non-empty set $E \subset \mathbb{N}$ and $c > 0$, we have

$$(12) \quad \limsup_{N \rightarrow \infty} \frac{|E \cap [N]|}{|E \cap [cN]|} > 0.$$

In fact, by contradiction, assume

$$\limsup_{N \rightarrow \infty} \frac{|E \cap [N]|}{|E \cap [cN]|} = 0.$$

Then there exists N_0 such that for all $N \geq N_0$, we have

$$\frac{|E \cap [N]|}{|E \cap [cN]|} < \frac{1}{2c}.$$

Or equivalently,

$$|E \cap [cN]| > 2c|E \cap [N]|.$$

Inductively, we have for all $n \in \mathbb{N}$,

$$(13) \quad |E \cap [c^n N_0]| > (2c)^n |E \cap [N_0]|.$$

But since $|E \cap [c^n N_0]| \leq c^n N_0$, (13) cannot hold for n very large. This is a contradiction. This finishes the proof of the claim.

We now return to the proof of Lemma 5.1. Since S is syndetic in G , there exists a finite subset $F \subset G$ such that $S/F = G$. It follows that

$$\sum_{m \in F} 1_S(mn) \geq 1 \quad \text{for all } n \in G.$$

Therefore

$$(14) \quad \sum_{n \in [N] \cap G} \sum_{m \in F} 1_S(mn) \geq |G \cap [N]|.$$

Let $M = \max\{m : m \in F\}$. Since each $n \leq MN$ is repeated at most $|F|$ times in the sum appearing in the left hand side of (14), we deduce that

$$\sum_{n \in G \cap [MN]} 1_S(n) \geq \frac{|G \cap [N]|}{|F|}.$$

Therefore

$$(15) \quad \mathbb{E}_{n \in G \cap [MN]} 1_S(n) \geq \frac{|G \cap [N]|}{|F||G \cap [MN]|}$$

In view of the claim,

$$(16) \quad \limsup_{N \rightarrow \infty} \frac{|G \cap [N]|}{|G \cap [MN]|} > 0.$$

(16) and (15) imply $\bar{d}_G(S) > 0$.

Assume G has positive lower additive density. In this case, we have

$$\frac{|G \cap [N]|}{|G \cap [MN]|} = \frac{|G \cap [N]|}{N} \cdot \frac{N}{|G \cap [MN]|} \geq \frac{\delta}{M} \text{ for sufficiently large } N.$$

Hence, for sufficiently large N ,

$$(17) \quad \mathbb{E}_{n \in G \cap [MN]} 1_S(n) \geq \frac{\delta}{M|F|}.$$

We now have

$$(18) \quad \mathbb{E}_{n \in G \cap [N]} 1_S(n) = \frac{1}{|G \cap [N]|} \sum_{n \in G \cap [N]} 1_S(n) \geq \frac{|G \cap [M \lfloor N/M \rfloor]|}{|G \cap [N]|} \cdot \frac{1}{|G \cap [M \lfloor N/M \rfloor]|} \sum_{n \in G \cap [M \lfloor N/M \rfloor]} 1_S(n) = \frac{|G \cap [M \lfloor N/M \rfloor]|}{|G \cap [N]|} \mathbb{E}_{n \in G \cap [M \lfloor N/M \rfloor]} 1_S(n).$$

Moreover,

$$(19) \quad \frac{|G \cap [M \lfloor N/M \rfloor]|}{|G \cap [N]|} \geq \frac{|G \cap [M \lfloor N/M \rfloor]|}{M \lfloor N/M \rfloor} \cdot \frac{M \lfloor N/M \rfloor}{N} > \frac{|G \cap [M \lfloor N/M \rfloor]|}{M \lfloor N/M \rfloor} \cdot \frac{M(N/M - 1)}{N} > \frac{\delta}{2}$$

for sufficiently large N . Combining (17), (18) and (19), for sufficiently large N ,

$$\mathbb{E}_{n \in G \cap [N]} 1_S(n) > \frac{\delta^2}{2M|F|}$$

This implies $d_G(S) > 0$. This finishes our proof. \square

Remark 5.2. Lemma 5.1 implies that a multiplicatively syndetic set in \mathbb{N} has positive upper density. On the contrary, it is not true that an additively syndetic set has positive upper multiplicative density. For example, the set $2\mathbb{N} + 1$ is additively syndetic but has zero multiplicative density with respect to any multiplicative Følner sequence.

It is worth noting that in (12), one can not replace \limsup with \liminf . In fact, we have:

Proposition 5.3. *There exists a subsemigroup G of (\mathbb{N}, \times) such that*

$$\liminf_{N \rightarrow \infty} \frac{|G \cap [N]|}{|G \cap [2N]|} = 0.$$

Proof. We construct G by putting primes into G in an inductive way as follows. Let $1 \leq N_1 < N_2 < \dots$ be a sequence of integers with the exact values of N_k to be chosen later. Put all primes in the intervals $[N_1, 2N_1] \cup [N_2, 2N_2] \cup \dots$ into G . Other elements of G are generated from those primes. Then for $k \in \mathbb{N}$, the set $G \cap [N_{k+1}]$ is subset of the set $\{p_1^{\ell_1} \cdots p_m^{\ell_m} : p_1, \dots, p_m \in \mathbb{P} \cap [N_k], m \in \mathbb{N}\}$ where \mathbb{P} denotes the set of primes. Since $|\mathbb{P} \cap N_k| < N_k$, we can see

$$|G \cap [N_{k+1}]| < (\log_2 N_{k+1})^{N_k} < (2 \log N_{k+1})^{N_k}.$$

On the other hand, using the Prime Number Theorem, we have

$$|G \cap [N_{k+1}, 2N_{k+1}]| \geq |\mathbb{P} \cap [N_{k+1}, 2N_{k+1}]| = \frac{N_{k+1}}{\log N_{k+1}} (1 + o_{k \rightarrow \infty}(1))$$

Hence

$$(20) \quad \frac{|G \cap [N_{k+1}]|}{|G \cap [N_{k+1}, 2N_{k+1}]|} \leq \frac{(2 \log N_{k+1})^{N_{k+1}}}{N_{k+1}} (1 + o_{k \rightarrow \infty}(1))$$

If we choose the sequence (N_k) growing fast enough so that the quantity on the right hand side of (20) approaches zero as $k \rightarrow \infty$, then we have the conclusion. \square

5.2. Averages along subsemigroups of (\mathbb{N}, \times) . Theorem 1.3 now follows from the next result.

Theorem 5.4. *Let (X, \mathcal{B}, μ, T) be a measure preserving (\mathbb{N}, \times) -system and $A \in \mathcal{B}$ with $\mu(A) > 0$. Let (G, \times) be a subsemigroup of (\mathbb{N}, \times) . Then for every $\ell \in \mathbb{N}$,*

$$\limsup_{N \rightarrow \infty} \mathbb{E}_{n \in G \cap [N]} \mu(A \cap T_n^{-1} A \cap \dots \cap T_{n^\ell}^{-1} A) > 0.$$

If $\liminf_{N \rightarrow \infty} \frac{|G \cap [N]|}{N} > 0$ (i.e. G has positive lower density), then we have the stronger bound

$$\liminf_{N \rightarrow \infty} \mathbb{E}_{n \in G \cap [N]} \mu(A \cap T_n^{-1} A \cap \dots \cap T_{n^\ell}^{-1} A) > 0.$$

Remark 5.5. Theorem 5.4 is no longer true if we replace the Følner sequence $([N])_{N \in \mathbb{N}}$ by arbitrary additive Følner sequence on \mathbb{N} . For example, take (X, \mathcal{B}, μ, T) to be the (\mathbb{N}, \times) -system where $X = \mathbb{T}$, μ is the Lebesgue measure and $T_n x := x + \log n$, and let A be a small interval on X . Then there exist arbitrary long intervals $[M, N)$ of integers such that $A \cap T_n^{-1} A = \emptyset$ for all $n \in [M, N)$. Therefore we can find a Følner sequence Φ consisting of longer and longer such intervals with the property that

$$\lim_{N \rightarrow \infty} \mathbb{E}_{n \in \Phi_N} \mu(A \cap T_n A) = 0.$$

Proof. In view of Theorem 2.3, there exists $\delta > 0$ such that the set

$$S = \{n \in G : \mu(A \cap T_n^{-1}A \cap \dots \cap T_{n^\ell}^{-1}A) > \delta\}$$

is syndetic in (G, \times) . We then have

$$\mathbb{E}_{n \in G \cap [N]} \mu(A \cap T_n^{-1}A \cap \dots \cap T_{n^\ell}^{-1}A) \geq \delta \mathbb{E}_{n \in G \cap [N]} 1_S.$$

Theorem 5.4 now follows from Lemma 5.1. \square

We conclude this section by remarking that one can not replace the lim inf and lim sup in Theorem 5.4 with limits. This is because the limits may not exist as the following proposition shows.

Proposition 5.6. *There exists a measure preserving system (\mathbb{N}, \times) -system (X, \mathcal{B}, μ, T) and a set $A \in \mathcal{B}$ such that*

$$(21) \quad \lim_{N \rightarrow \infty} \mathbb{E}_{n \in [N]} \mu(A \cap T_n^{-1}A)$$

does not exist.

Proof. Let $\chi: \mathbb{N} \rightarrow S^1$ be the completely multiplicative function $\chi(n) = n^i = e^{i \log n}$ for $n \in \mathbb{N}$. It is well known that

$$(22) \quad \lim_{N \rightarrow \infty} \mathbb{E}_{n \in [N]} \chi(n)$$

does not exist. Consider the (\mathbb{N}, \times) -system $(X = S^1, \mu, (T_n)_{n \in \mathbb{N}})$ where μ is the normalized Lebesgue measure on X and $T_n(x) := \chi(n)x$ for $x \in X$ and $n \in \mathbb{N}$. We show that this system satisfies our condition. By contradiction, assume for every $A \subset X$ measurable, the limit in (21) exists.

Let A be an arbitrary measurable subset of X . Let \mathcal{H} be the smallest closed subspace of $L^2(X)$ that contains $T_n 1_A$ for all $n \in \mathbb{N}$ and constant functions. By our assumption, for every $g \in \mathcal{H}$,

$$\lim_{N \rightarrow \infty} \mathbb{E}_{n \in [N]} \int_X 1_A(T_n x) \bar{g}(x) d\mu(x)$$

exists. Let

$$\mathcal{F} = \left\{ f \in L^2(X) : \lim_{N \rightarrow \infty} \mathbb{E}_{n \in [N]} \int_X 1_A(T_n x) \cdot \bar{f}(x) d\mu(x) \text{ exists} \right\}.$$

It follows that $\mathcal{H} \subset \mathcal{F}$. On the other hand, for all $g \in \mathcal{H}^\perp$, we have

$$\int_X 1_A(T_n x) \cdot \bar{g}(x) d\mu(x) = 0.$$

Hence

$$\lim_{N \rightarrow \infty} \mathbb{E}_{n \in [N]} \int_X 1_A(T_n x) \cdot \bar{g}(x) d\mu(x)$$

exists and is equal to 0. In particular, $\mathcal{H}^\perp \subset \mathcal{F}$. Therefore $\mathcal{F} = L^2(X)$. In conclusion, for every $A \in \mathcal{B}$ and every $f \in L^2(X)$, the limit

$$\lim_{N \rightarrow \infty} \mathbb{E}_{n \in [N]} \int_X 1_A(T_n x) \cdot \bar{f}(x) \mu(x)$$

exists. By approximating f with simple functions, we get for all $f \in L^2(X)$, the limit

$$\lim_{N \rightarrow \infty} \mathbb{E}_{n \in [N]} \int_X f(T_n x) \cdot \bar{f}(x) \mu(x)$$

exists. However, this is not true as the following example shows. Let $f: X \rightarrow \mathbb{C}$ be defined by $f(x) = x$ for $x \in S^1$. Then $f(T_n x) = \chi(n)x$. We then have

$$\int_X f(T_n x) \bar{f}(x) d\mu = \chi(n).$$

Hence the limit

$$(23) \quad \lim_{N \rightarrow \infty} \mathbb{E}_{n \in [N]} \int_X f \cdot T_n \bar{f} d\mu$$

does not exist. We reach a desired contradiction. \square

Remark 5.7. One may ask whether the limit in (21) might exist after replacing Cesàro averages with a different averaging scheme (for example logarithmic averages). However, for any given averaging scheme, there exists a complete multiplicative function χ for which the limit in (22) does not exist. Hence we can carry a similar construction as in proof of Proposition 5.6 to show that there exists a system and set A for which the limit in (21) with respect to such an averaging scheme does not exist.

5.3. Subordinated semigroups. In this section, we introduce the notion of subordinated semigroups of $(\mathbb{N}^k, *)$ and some basic properties of these semigroups for later uses.

Definition 5.8 (Subordinated semigroups). We say that a semigroup $(\mathbb{N}^k, *)$ is *subordinated* to the Euclidean norm $\|\cdot\|$ in \mathbb{N}^k if there exists a constant $C > 0$ such that

$$(24) \quad \|n * m\| \leq C \|n\| \|m\| \text{ for all } n, m \in \mathbb{N}^k.$$

We remark that (24) is equivalent of saying that $\sup_{n, m \in \mathbb{N}^k} \frac{\|n * m\|}{\|n\| \|m\|}$ is finite. Also note that, up to modifying the constant C , in the definition of subordinated semigroup we may change the Euclidean norm $\|\cdot\|$ by any other equivalent norm.

The following lemma follows immediately from the definition.

Lemma 5.9. *Let $(\mathbb{N}^k, *)$ be a semigroup subordinated to the Euclidean norm in \mathbb{N}^k . Then for every $m \in \mathbb{N}^k$, there exists $K = K(m) \in \mathbb{N}$ such that for all $N \in \mathbb{N}$ and $n \in \mathbb{N}^k$ with $\|n\| \leq N$, we have that $\|m * n\| \leq KN$.*

A class of subordinated semigroups of particular interest for us is given by semigroups $(\mathbb{N}^k, *)$ whose operation is induced by the usual matrix multiplication in a subsemigroup of $\mathcal{M}_{d \times d}(\mathbb{Z})$ for some $d \in \mathbb{N}$. Here $\mathcal{M}_{d \times d}(\mathbb{Z})$ denotes the set of $d \times d$ -matrices with integer coefficients.

Definition 5.10. Let $d, k \in \mathbb{N}$. We say that a semigroup $(\mathbb{N}^k, *)$ is induced by $\mathcal{M}_{d \times d}(\mathbb{Z})$ (via ψ) if there exists a linear injection $\psi: \mathbb{N}^k \rightarrow \mathcal{M}_{d \times d}(\mathbb{Z})$ (meaning that ψ is a linear function of \mathbb{N}^k in every entry) such that $\psi(\mathbb{N}^k)$ is a semigroup of $\mathcal{M}_{d \times d}(\mathbb{Z})$ not contained in $\{A \in \mathcal{M}_{d \times d}(\mathbb{Z}) : \det(A) = 0\}$ and such that

$$n * m = \psi^{-1}(\psi(n)\psi(m)).$$

Lemma 5.11. *A semigroup $(\mathbb{N}^k, *)$ induced by $\mathcal{M}_{d \times d}(\mathbb{Z})$ is subordinated to the Euclidean norm in \mathbb{N}^k .*

Proof. We regard $\mathcal{M}_{d \times d}(\mathbb{Z})$ as a subset of \mathbb{R}^{d^2} , and let $N \in M_{k, d^2}(\mathbb{R})$ and $M \in M_{d^2, k}(\mathbb{R})$ be such that $\psi(x) = Nx$ and $\psi^{-1}(y) = My$ for $x \in \mathbb{N}^k$, $y \in \psi(\mathbb{N}^k)$. For any matrix $A \in M_{d_1, d_2}(\mathbb{R})$, denote $\|A\| = \sup_{x \in \mathbb{R}^{d_1} \setminus \{0\}} \|Ax\|/\|x\|$. We have that

$$\|n * m\| = \|\psi^{-1}(\psi(n) \cdot \psi(m))\| \leq \|M\| \|\psi(n) \cdot \psi(m)\| \leq \|M\| \|\psi(n)\| \|\psi(m)\| \leq \|M\| \|N\|^2 \|n\| \|m\|.$$

□

The next lemma states that a (multiplicative) syndetic subset in a semigroup subordinated to the Euclidean norm has positive (additive) lower density; this phenomenon was already observed in Lemma 5.1.

Lemma 5.12. *Let $(\mathbb{N}^k, *)$ be a semigroup subordinated to the Euclidean norm in \mathbb{N}^k and $(Z, *)$ be a subsemigroup of $(\mathbb{N}^k, *)$ with*

$$\bar{d}_+(Z) := \limsup_{N \rightarrow \infty} \frac{|[N]^k \cap Z|}{N^k} = 1.$$

Let $S \subseteq Z$ be a syndetic subset (with respect to the $$ operation). Then,*

$$\liminf_{N \rightarrow \infty} \mathbb{E}_{n \in [N]^k \cap Z} 1_S(n) > 0.$$

Proof. Since S is syndetic, there exists a finite set $F \subset Z$ such that $Z = F^{-1} * S$. Then for every $x \in Z$ we have that $1 \leq \sum_{n \in F} 1_S(n * x)$. By Lemma 5.9, there exist $K = \max\{K(n) : n \in$

$F\}$ and $N_0 := \max\{N_0(n) : n \in F\}$ such that for all $N \geq N_0$, $m * n \in f([KN]^k)$ for all $n \in [N]^k$ and $m \in F$. So for all $N \geq N_0$,

$$1 \leq \liminf_{N \rightarrow \infty} \mathbb{E}_{n \in [N]^k \cap Z} \sum_{m \in F} 1_S(m * n) = \liminf_{N \rightarrow \infty} \sum_{m \in F} \mathbb{E}_{n \in [N]^k \cap Z} 1_S(m * n) \leq \liminf_{N \rightarrow \infty} \frac{1}{N^k} \sum_{n \in [KN]^k \cap Z} 1_S(n),$$

where in the last inequality we used the fact that the map $n \rightarrow m * n$ is injective from Z to Z for all $m \in Z$. Therefore,

$$(25) \quad \liminf_{N \rightarrow \infty} \mathbb{E}_{n \in [mN]^k \cap Z} 1_S(n) > K^{-k} > 0.$$

Now for all $N \geq KN_0$, let $M = \lceil N/K \rceil$, then (25) implies that

$$\begin{aligned} \liminf_{N \rightarrow \infty} \mathbb{E}_{n \in [N]^k \cap Z} 1_S(n) &\geq \liminf_{N \rightarrow \infty} \left(\frac{KM}{N}\right)^k \mathbb{E}_{n \in [KM]^k \cap Z} 1_S(n) \\ &> \liminf_{N \rightarrow \infty} \left(\frac{KM}{N}\right)^k K^{-k} > \liminf_{N \rightarrow \infty} \left(\frac{1}{K} - \frac{1}{N}\right)^k. \end{aligned}$$

So $\liminf_{N \rightarrow \infty} \mathbb{E}_{n \in [N]^k \cap Z} 1_S(n) \geq K^{-k}$ and we are done. \square

5.4. Parametrized multiplicative functions. In this section, we introduce a class of functions that parametrize multiplicative subsemigroups of $\mathbb{Q}^{>0}$.

Definition 5.13 (Parametrized multiplicative function). For $k \in \mathbb{N}$, we say that $f : \mathbb{N}^k \rightarrow \mathbb{Q}^{\geq 0}$ is a *parametrized multiplicative function* if

$$\bar{d}_+(\{n \in \mathbb{N}^k : f(n) = 0\}) = 0$$

and there exists an operation $*$: $\mathbb{N}^k \times \mathbb{N}^k \rightarrow \mathbb{N}^k$ so that $(\mathbb{N}^k, *)$ is a semigroup subordinated to the euclidean norm in \mathbb{N}^k and

$$f(n * m) = f(n)f(m)$$

for all $n, m \in \mathbb{N}^k$. We say that f is a *commutative parametrized multiplicative function* if one can choose $(\mathbb{N}^k, *)$ to be a cancelative commutative semigroup.

Remark 5.14. We could disallow functions $f : \mathbb{N}^k \rightarrow \mathbb{Q}^{\geq 0}$ that take the value 0, but this would forbid some of the natural examples we exhibit below. On the other hand, we are interested in functions that take values in the multiplicative group $(\mathbb{Q}^{>0}, \times)$, so as a compromise we allow parametrized multiplicative functions to take the value 0, as long as only on a set of zero additive density.

This definition leads to a situation where we may have a function $f : \mathbb{N}^k \rightarrow \mathbb{R}$ which is only defined on a full density subset D of \mathbb{N}^k ; in such cases we denote by

$$\liminf_{N \rightarrow \infty} \mathbb{E}_{n \in [N]^k} f(n) := \liminf_{N \rightarrow \infty} \mathbb{E}_{n \in [N]^k} 1_D(n) f(n).$$

We sometimes write $f: (\mathbb{N}^k, *) \rightarrow \mathbb{Q}^{\geq 0}$ for a parametrized multiplicative function to stress the semigroup operation for which f is a multiplicative function.

A typical example of a parametrized multiplicative function arising from a semigroup $(\mathbb{N}^k, *)$ induced by $\mathcal{M}_{d \times d}(\mathbb{Z})$ is the one induced by the determinant function. That is $f: (\mathbb{N}^k, *) \rightarrow \mathbb{Q}^{\geq 0}$, $n \mapsto |\det(\psi(n))|$, or more generally $n \mapsto \xi(|\det(\psi(n))|)$ for any multiplicative function $\xi: |\det(\psi(\mathbb{N}^k))| \rightarrow \mathbb{Q}^{\geq 0}$. Here we point out that since $\psi(\mathbb{N}^k)$ is not contained in $\{A \in \mathcal{M}_{d \times d}(\mathbb{Z}) : \det(A) = 0\}$, the polynomial $\det(\psi(n))$ is non trivial and therefore $\bar{d}(\{n \in \mathbb{N}^k : \det(\psi(n)) = 0\}) = 0$. (To see this, note that for $(n_1, \dots, n_{k-1}) \in \mathbb{N}^{k-1}$ there are at most d positive integers $n_k \in \mathbb{N}$ such that $\det(\psi(n_1, \dots, n_{k-1}, n_k)) = 0$.)

Example 5.15. In the following, we present some examples of parametrized multiplicative functions.

- (1) Consider the function f given by $f = \det \circ \psi$, where $\psi: \mathbb{N}^2 \rightarrow \mathcal{M}_{2 \times 2}(\mathbb{Z})$, $(n_1, n_2) \mapsto \begin{pmatrix} n_1 & -n_2 \\ n_2 & n_1 \end{pmatrix}$ is a linear injection. By Lemma 5.11, the semigroup induced by $\mathcal{M}_{2 \times 2}(\mathbb{Z})$ via ψ is subordinated to the Euclidean norm in \mathbb{N}^2 . Thus we have that $f(n_1, n_2) = n_1^2 + n_2^2$ is a parametrized multiplicative function.
- (2) If $k = a^2 + b^2$ for some $a, b \in \mathbb{N}$, then $f(n_1, n_2) = k(n_1^2 + n_2^2)$ is a parametrized multiplicative function, since $f = \det \circ \psi$ with $\psi: \mathbb{N}^2 \rightarrow \mathcal{M}_{2 \times 2}(\mathbb{Z})$ being the linear injection $(n_1, n_2) \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} n_1 & -n_2 \\ n_2 & n_1 \end{pmatrix}$.
- (3) Similar to the previous examples, the linear injection $\psi: (n_1, n_2) \mapsto \begin{pmatrix} n_1 & -Dn_2 \\ n_2 & n_1 \end{pmatrix}$ for $D \in \mathbb{Z}$ gives us the parametrized multiplicative function $f(n_1, n_2) = |\det \circ \psi(n_1, n_2)| = |n_1^2 + Dn_2^2|$.
- (4) Given two parametrized multiplicative functions, $f_1: (\mathbb{N}^{d_1}, *_1) \rightarrow \mathbb{Q}^{\geq 0}$ and $f_2: (\mathbb{N}^{d_2}, *_2) \rightarrow \mathbb{Q}^{\geq 0}$, we may define for $\ell_1, \ell_2 \in \mathbb{Z}$ the function $f: (\mathbb{N}^{d_1} \times \mathbb{N}^{d_2}, *_1 \times *_2) \rightarrow \mathbb{Q}$, such that $f(n_1, n_2) = f_1^{\ell_1}(n_1) f_2^{\ell_2}(n_2)$, if $f_1(n_1) f_2(n_2) \neq 0$ and $f(n_1, n_2) = 0$ otherwise. Since $(\mathbb{N}^{d_i}, *_i)$, $i = 1, 2$ is subordinated to the Euclidean norm in \mathbb{N}^{d_i} , we get that $(\mathbb{N}^{d_1} \times \mathbb{N}^{d_2}, *_1 \times *_2)$ is subordinated to the Euclidean norm in $\mathbb{N}^{d_1} \times \mathbb{N}^{d_2}$. It is not hard to check that the upper density of $\{(n_1, n_2) \in \mathbb{N}^{d_1} \times \mathbb{N}^{d_2} : f(n_1, n_2) = 0\}$ equals 0. This implies that f is a parametrized multiplicative function. This also shows that $1/f_1$ is a parametrized multiplicative function.

In particular, for any $p, q \in \mathbb{Z}$ the function $f: \mathbb{N}^2 \rightarrow \mathbb{Q}^{>0}$, $(m, n) \mapsto m^p n^q$ is a parametrized multiplicative function.

- (5) Let K be a finite field extension of \mathbb{Q} and \mathcal{O}_K be the ring of integers of K . Let $d = [K : \mathbb{Q}]$ and $\mathcal{B} = \{b_1, \dots, b_d\}$ be an integral basis of \mathcal{O}_K , i.e., every $x \in \mathcal{O}_K$ can be

written as $x = n_1b_1 + \cdots + n_db_d$ for some $n_1, \dots, n_d \in \mathbb{Z}$ in a unique way. Let $N_K(x)$ denote the norm of x in K . Since $N_K(x)N_K(y) = N_K(xy)$, the function $f: \mathbb{N}^d \rightarrow \mathbb{Q}^{>0}$ given by $f(n_1, \dots, n_d) = |N_K(n_1b_1 + \cdots + n_db_d)|$ is a parametrized multiplicative function. We remark that in this example, f can be written as $f = \det \circ \psi$ for some linear injection $\psi: \mathbb{Z}^d \rightarrow \mathcal{M}_{d \times d}(\mathbb{Q})$.

As a special case, let $\omega = e^{2\pi i/3}$ and $K = \mathbb{Q}(\omega)$. Then $\{1, \omega, \omega^2\}$ is an integral basis of \mathcal{O}_K . For every $x = a_0 + a_1\omega + a_2\omega^2$ and $y = b_0 + b_1\omega + b_2\omega^2$ with $a_0, a_1, a_2, b_0, b_1, b_2 \in \mathbb{Q}$, note that

$$\begin{aligned} xy &= (a_0b_0 + a_1b_2 + a_2b_1) + (a_0b_1 + a_1b_0 + a_2b_2)\omega + (a_1b_1 + a_0b_2 + a_2b_0)\omega^2 \\ &= \begin{pmatrix} b_0 & b_1 & b_2 \end{pmatrix} \cdot \begin{pmatrix} a_0 & a_1 & a_2 \\ a_2 & a_0 & a_1 \\ a_1 & a_2 & a_0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ \omega \\ \omega^2 \end{pmatrix}. \end{aligned}$$

Therefore the function

$$\begin{aligned} f(a_0, a_1, a_2) &:= |N_K(a_0 + a_1\omega + a_2\omega^2)| = \left| \det \begin{pmatrix} a_0 & a_1 & a_2 \\ a_2 & a_0 & a_1 \\ a_1 & a_2 & a_0 \end{pmatrix} \right| \\ &= |(a_0 + a_1 + a_2)(a_0^2 + a_1^2 + a_2^2 - a_0a_1 - a_0a_2 - a_1a_2)| = |a_0^3 + a_1^3 + a_2^3 - 3a_0a_1a_2| \end{aligned}$$

is a parametrized multiplicative function.

- (6) Let $p: \mathbb{Z} \rightarrow \mathbb{Z}$ be the minimal polynomial of $A \in \mathcal{M}_{n \times n}(\mathbb{Z})$ and $d = \deg(p)$. Let $\psi: \mathbb{N}^d \rightarrow \mathcal{M}_{n \times n}(\mathbb{Z})$ be such that $\psi(n_0, \dots, n_{d-1}) := n_0I_n + n_1A + \cdots + n_{d-1}A^{d-1}$ (which is a linear injection since d is the degree of the minimal polynomial of A). Since $p(A) = 0$, $\psi(\mathbb{N}^d)$ is a semigroup and $\psi^{-1}: \psi(\mathbb{N}^d) \rightarrow \mathbb{N}$ is a well defined map. So we may denote

$$n * m := \psi^{-1}(\psi(n)\psi(m)).$$

Also note that $\psi(\mathbb{N}^d)$ does not consists of only non-invertible matrices. Then the group $(\mathbb{N}^d, *)$ is induced by $\mathcal{M}_{n \times n}(\mathbb{Z})$ (via the map ψ), and so $|\det \circ \psi|: \mathbb{N}^d \rightarrow \mathbb{Z}$ is a parametrized multiplicative function.

To illustrate this class of examples, consider the Fibonacci matrix $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Its minimal polynomial is of degree 2 and then we can consider $\psi: \mathbb{N}^2 \rightarrow \mathcal{M}_{2 \times 2}(\mathbb{Z})$, given by

$$\psi(n, m) = nI + mA = \begin{pmatrix} n+m & m \\ m & n \end{pmatrix}$$

Hence $|\det \circ \psi(n, m)| = |n^2 - m^2 + nm|$ is a parametrized multiplicative function.

More generally, consider a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ not being a multiple of the identity.

Then its minimal polynomial is of degree 2 and therefore

$$|\det(nI + mA)| = \left| \det \begin{pmatrix} n + am & bm \\ cm & n + dm \end{pmatrix} \right| = |n^2 + (a + d)mn + (ad - bc)m^2|$$

is a parametrized multiplicative function.

- (7) Consider the quaternion semigroup of matrices $\{M_{n_1, n_2, n_3, n_4} : n_1, n_2, n_3, n_4 \in \mathbb{N}\}$ where

$$M_{n_1, n_2, n_3, n_4} = \begin{pmatrix} n_1 & -n_2 & -n_3 & -n_4 \\ n_2 & n_1 & -n_4 & n_3 \\ n_3 & n_4 & n_1 & -n_2 \\ n_4 & -n_3 & n_2 & n_1 \end{pmatrix}.$$

Via the linear injection $\psi: \mathbb{N}^4 \rightarrow \mathcal{M}_{4 \times 4}(\mathbb{Z})$ with $(n_1, n_2, n_3, n_4) \mapsto M_{n_1, n_2, n_3, n_4}$ we obtain the parametrized multiplicative functions $f(n_1, n_2, n_3, n_4) = \det \circ \psi(n_1, n_2, n_3, n_4) = (n_1^2 + n_2^2 + n_3^2 + n_4^2)^2$ and $g(n_1, n_2, n_3, n_4) = (\det)^{1/2}(\psi(n_1, n_2, n_3, n_4)) = n_1^2 + n_2^2 + n_3^2 + n_4^2$.

We remark that the functions in examples (1)–(6) are all *commutative* parametrized multiplicative functions, however it is not clear whether the one in example (7) is, as the quaternion semigroup is non-commutative.

5.5. Averages along parametrized multiplicative functions. In this section we prove Theorem 1.4. In fact we will establish the following more general version which also deals with commutative parametrized functions that take values in $\mathbb{Q}^{\geq 0}$. Recall the convention adopted in Remark 5.14.

Theorem 5.16. *Let (X, \mathcal{B}, μ, T) be a measure preserving (\mathbb{N}, \times) -system and $A \in \mathcal{B}$ with $\mu(A) > 0$. Let $f: \mathbb{N}^k \rightarrow \mathbb{Q}^{\geq 0}$ be a commutative parametrized multiplicative function and $\ell \in \mathbb{N}$. Then*

$$\liminf_{N \rightarrow \infty} \mathbb{E}_{n \in [N]^k} \mu \left(A \cap T_{f(n)}^{-1} A \cap T_{f(n)^2}^{-1} A \cap \dots \cap T_{f(n)^\ell}^{-1} A \right) > 0.$$

Proof. The proof resembles that of Theorem 5.4. Let $(\mathbb{N}^k, *)$ be the semigroup that gives rise to the parametrized multiplicative function f . Let Z be the set of all $n \in \mathbb{N}^k$ with $f(n) > 0$. Since f is a homomorphism, $(Z, *)$ is a subsemigroup of $(\mathbb{N}^k, *)$. For each $n \in Z$, let $R_n := T_{f(n)}$. Denote by n^{*k} the iterate product $n^{*k} = n * n \dots * n$ (k -times). By Theorem 2.3, there exists $\delta > 0$ such that the set

$$S = \{n \in Z : \mu(A \cap R_n^{-1} A \cap \dots \cap R_{n^{*\ell}}^{-1} A) > \delta\}$$

is syndetic in $(Z, *)$. Since $\bar{d}_+(Z) = 1$ by definition, we have

$$\begin{aligned} & \liminf_{N \rightarrow \infty} \mathbb{E}_{n \in [N]^k} \mu(A \cap T_{f(n)}^{-1} A \cap T_{f(n)^2}^{-1} A \cap \cdots \cap T_{f(n)^\ell}^{-1} A) \\ &= \liminf_{N \rightarrow \infty} \mathbb{E}_{n \in [N]^k \cap Z} \mu(A \cap T_{f(n)}^{-1} A \cap T_{f(n)^2}^{-1} A \cap \cdots \cap T_{f(n)^\ell}^{-1} A) \\ &\geq \delta \liminf_{N \rightarrow \infty} \mathbb{E}_{n \in [N]^k \cap Z} 1_S(n) > 0, \end{aligned}$$

where the last inequality comes from Lemma 5.12. \square

As an immediate corollary of Theorem 1.4, we conclude that for all multiplicative measure preserving system (X, \mathcal{B}, μ, T) and $A \in \mathcal{B}$ with $\mu(A) > 0$, the following averages are positive:

- (1) $\liminf_{N \rightarrow \infty} \mathbb{E}_{m, n \in [N]} \mu(T_{m^a}^{-1} A \cap T_{n^b}^{-1} A)$ for $a, b \in \mathbb{N}$;³
- (2) $\liminf_{N \rightarrow \infty} \mathbb{E}_{n, m \in [N]} \mu(A \cap T_{n^2+m^2}^{-1} A)$ (which implies Proposition 1.5);
- (3) $\liminf_{N \rightarrow \infty} \mathbb{E}_{n, m \in [N]} \mu(A \cap T_{n^2+Dm^2}^{-1} A)$ for all $D \in \mathbb{N}$;
- (4) $\liminf_{N \rightarrow \infty} \mathbb{E}_{n, m \in [N]} \mu(A \cap T_{k(n^2+m^2)}^{-1} A \cap T_{(k(n^2+m^2))^2} A)$ for all k of the form $a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Remark 5.17. We remark that item (4) above fails if k does not have the form $a^2 + b^2$. Indeed, if this is the case, there exists a prime $p \equiv 3 \pmod{4}$ such that p has odd exponent in prime factorization of k . For $n \in \mathbb{N}$ let $f_p(n)$ denote the exponent of p in the prime factorization of n . We then have $f_p(k(m^2 + n^2))$ is odd for all $m, n \in \mathbb{N}$. For $n \in \mathbb{N}$, color n with $C(n) \equiv f_p(n) \pmod{2}$. It follows that $\{k(m^2 + n^2) : m, n \in \mathbb{N}\}$ is not a set of topological multiplicative recurrence.

5.6. Single recurrence and non-commutative semigroups. Next theorem shows that in the special case $\ell = 1$ of Theorem 1.4, one can drop the assumption that f arises from a commutative semigroup.

Theorem 5.18. *Let (X, \mathcal{B}, μ, T) be an (\mathbb{N}, \times) measure preserving system and $A \in \mathcal{B}$ with $\mu(A) > 0$. Let $f: (\mathbb{N}^k, *) \rightarrow \mathbb{Q}^{\geq 0}$ be a parametrized multiplicative function. Then*

$$\liminf_{N \rightarrow \infty} \mathbb{E}_{n \in [N]^k} \mu(A \cap T_{f(n)}^{-1} A) > 0.$$

Proof. Let $(\mathbb{N}^k, *)$ be the semigroup that gives the parametrized multiplicative function f . Let Z be the set of all $n \in \mathbb{N}^k$ with $f(n) > 0$. Since f is a homomorphism, $(Z, *)$ is a subsemigroup of $(\mathbb{N}^k, *)$. For $n \in Z$, denote $R_n := T_{f(n)}$. By Theorem 2.4, the set

$$S := \{n \in Z : \mu(A \cap R^n A) > \mu^2(A)/2\}$$

³We do not know how to establish this without using Theorem 1.4 (i.e. using only Theorem 1.3).

is syndetic in $(Z, *)$. Since $\mu(A \cap R^n A) \geq \frac{1}{2}\mu(A)^2 1_S(n)$ for all $n \in Z$ and $\bar{d}_+(Z) = 1$, it suffices to show that

$$\liminf_{N \rightarrow \infty} \mathbb{E}_{n \in [N]^k \cap Z} 1_S(n) > 0.$$

The last inequality follows from Lemma 5.12, so our proof finishes. \square

Remark 5.19. As an immediate corollary of Theorem 5.18, we conclude that for all measure preserving (\mathbb{N}, \times) -system (X, \mathcal{B}, μ, T) and $A \in \mathcal{B}$ with $\mu(A) > 0$,

$$\liminf_{N \rightarrow \infty} \mathbb{E}_{n_1, n_2, n_3, n_4 \in [N]} \mu(A \cap T_{n_1^2 + n_2^2 + n_3^2 + n_4^2}^{-1} A) > 0.$$

6. DENSITY REGULARITY OF PYTHAGOREAN TRIPLES IN FINITE FIELDS

6.1. Pythagorean pairs in finite fields. In what follows we explore the question of finding Pythagorean pairs in sets of positive density in finite fields. We start with a result in number theory, which follows from [21, Theorem 5A] (see also the proof of Corollary 5B there).

Theorem 6.1 ([21, Theorem 5A]). *Let $k \in \mathbb{N}$, let F be a finite field, let $Q = \{x^2 : x \in F\}$ and let $a_1, \dots, a_k \in F$ be arbitrary and pairwise distinct. Then*

$$\frac{|(Q - a_1) \cap \dots \cap (Q - a_k)|}{|F|} = \frac{1}{2^k} + o_{k, |F| \rightarrow \infty}(1).$$

In next proposition, we show that Conjecture 1.1 is true when \mathbb{N} is replaced by a finite field. In fact, we prove a stronger result which involves “density regularity” rather than “partition regularity”.

Proposition 6.2. *For every $\delta > 0$ there is $M > 0$ such that whenever \mathbb{F} is a finite field with $|\mathbb{F}| > M$ and $A \subset \mathbb{F}$ having $|A| > \delta|\mathbb{F}|$, there exist $x, y \in A$ with $x^2 + y^2$ being a perfect square.*

Proof. Since $|A| > \delta|\mathbb{F}|$, the set $B := \{x^2 : x \in A\}$ has $|B| > \frac{\delta}{2}|\mathbb{F}|$. Our task is to show that there exist $x, y \in B$ such that $x + y$ is a perfect square when $|\mathbb{F}|$ is sufficiently large. Denote by Q the set of perfect squares in \mathbb{F} ; we will show that there exists $x \in B$ such that $(Q - x) \cap B \neq \emptyset$. This will follow if we show that the set $Q_B := \bigcup_{x \in B} (Q - x)$ satisfies $|Q_B| > (1 - \delta/2)|\mathbb{F}|$.

Let $Q^c := \mathbb{F} \setminus Q$ and $Q_B^c := \mathbb{F} \setminus Q_B$. Then we have $Q_B^c = \bigcap_{x \in B} (Q^c - x)$ and we want to show that $|Q_B^c| < \frac{\delta}{2}|\mathbb{F}|$. Let $k \in \mathbb{N}$ be such that $1/2^k < \frac{\delta}{2}$. In view of Theorem 6.1, $|Q_B^c| = \frac{1}{2^k} + o_{k, |\mathbb{F}| \rightarrow \infty}(1)$, so if $|\mathbb{F}|$ is large enough we conclude that indeed $|Q_B^c| < \frac{\delta}{2}$, as desired. \square

Remark 6.3. In contrast to Proposition 6.2, it is not true that every set of positive additive density of \mathbb{N} contains x, y such that $x^2 + y^2$ is a perfect square. For example, consider the set $4\mathbb{N} + 1$.

6.2. Pythagorean triples in finite fields. It is also natural to ask whether an extension of Proposition 6.2 stating that there exist $x, y, z \in A$ with $x^2 + y^2 = z^2$ still holds. We show that this is false and characterize all equations of the form $ax^2 + by^2 + cz^2 = 0$ for which the analogous results are true.

Proposition 6.4. *For $a, b, c \in \mathbb{Z}$, the followings are equivalent:*

- (i) *For every $\delta > 0$, there is M such that whenever \mathbb{F} is a finite field with $|\mathbb{F}| > M$ and $A \subseteq \mathbb{F}$ with $|A| > \delta|\mathbb{F}|$, there exist $x, y, z \in A$ such that $ax^2 + by^2 + cz^2 = 0$.*
- (ii) $a + b + c = 0$.

Remark 6.5. We remark that related questions are also raised and addressed in [9, 19].

Proof. Suppose that $a + b + c = 0$ and \mathbb{F} is a finite field. Let $\delta > 0$ and $A \subset \mathbb{F}$ with $|A| > \delta|\mathbb{F}|$. Set $B := \{x^2 : x \in A\}$. Then $|B| \geq |A|/2 > \delta/2|\mathbb{F}|$. It suffices to find $x, t \in \mathbb{F}$ such that $x, x + ct, x - bt \in B$, but this immediately follows from Szemerédi Theorem for finite groups ([24, Theorem 10.5]).

Now assume that $a + b + c \neq 0$ and let $p > 2$ be a prime. Let $m = |a + b + c| > 0$ and q be the smallest prime such that $q > \max\{m, 5\}$. For $0 \leq i \leq m - 1$ and $0 \leq j \leq q - 1$, denote

$$B_{i,j} = \left\{ x \in \mathbb{Z} : iN/m \leq x < (i+1)p/m, x \equiv j \pmod{q} \text{ and } x \text{ is a perfect square } \pmod{p} \right\}$$

and let $A_{i,j} = \{x \in \mathbb{F} : x^2 \in B_{i,j}\}$. Then $\sum_{i=0}^{m-1} \sum_{j=0}^{q-1} |A_{i,j}| = p$.

We say that (i, j) is *good* if $mj \not\equiv ip \pmod{q}$. Let U be the set of (i, j) , $0 \leq i \leq m - 1$, $0 \leq j \leq q - 1$ which is good, and V be the set of (i, j) which is not good. Using the estimation $|A_{i,j}| \leq 2|B_{i,j}| \leq 2 + 2p/mq$ and the fact that $|V| \leq m$, we have that

$$\sum_{(i,j) \text{ is good}} |A_{i,j}| \geq p - 2m - 4p/q.$$

By the pigeonhole principle, if p is sufficiently large, then there exists a good pair (i, j) such that $|A_{i,j}| \geq (1 - 5/q)p/mq$. It suffices to show that $ax^2 + by^2 + cz^2 \neq 0$ for all $x, y, z \in A_{i,j}$.

Indeed, for any $x, y, z \in B_{i,j}$, denote $x' = mx - ip$, $y' = my - ip$ and $z' = mz - ip$. Then $0 \leq x', y', z' < p$. If $ax + by + cz = 0 \pmod{p}$, then $m(ax + by + cz) = 0 \pmod{p}$. By the construction of x', y' and z' , we have that $ax' + by' + cz' = 0 \pmod{p}$. Assume that $ax + by + cz = kp$ and $ax' + by' + cz' = rp$ for some $k, r \in \mathbb{Z}$, then $(mk - r)p = (a + b + c)ip = mip$. In other words, $mk - r = mi$. This implies that $m|r$. On the other hand, since $-mp < ax' + by' + cz' = rp < mp$, we must have that $r = 0$ and $ax' + by' + cz' = 0$. Therefore,

$$0 = ax' + by' + cz' \equiv (mj - ip)(a + b + c) = \pm m(mj - ip) \pmod{q}.$$

This is impossible since (i, j) is a good pair. This completes the proof. \square

Remark 6.6. An example due to Frantzikinakis shows that there exists a subset of \mathbb{N} of positive multiplicative density that contains no triple x, y, z such that $x^2 + y^2 = z^2$. The example is as follows: let $(\mathbb{T} := \mathbb{R}/\mathbb{Z}, \mu, T)$ be the multiplicative measure preserving system where μ is the Lebesgue measure and $T_n x = n^2 x$ for all $x \in \mathbb{T}$. Let x_0 be a generic point for μ . Fix $\delta > 0$ small. Then the set $E = \{n \in \mathbb{N} : n^2 x_0 \bmod 1 \in [1/2 - \delta, 1/2 + \delta]\}$ has multiplicative density $2\delta > 0$. For $x, y, z \in E$, $(x^2 + y^2)x_0 \bmod 1 \in [0, 2\delta] \cup [1 - 2\delta, 1)$ and $z^2 x_0 \in [1/2 - \delta, 1/2 + \delta]$. Hence $(x^2 + y^2)x_0 \neq z^2 x_0 \bmod 1$. It follows that $x^2 + y^2 \neq z^2$.

7. OPEN QUESTIONS

In this section, we collect some open questions regarding sets of multiplicative recurrence that naturally arise from our study. In [11, Problem 6], Frantzikinakis and Host ask whether the set $\{(m^2 + n^2)/m^2 : m, n \in \mathbb{N}\}$ is a set of topological multiplicative recurrence. In the spirit of this paper, we can ask the average version of this question, and some other related configurations:

Question 7.1. Let (X, \mathcal{B}, μ, T) be a multiplicative measure preserving system and $A \in \mathcal{B}$ with $\mu(A) > 0$. Is it true that

$$\liminf_{N \rightarrow \infty} \mathbb{E}_{n, m \in [N]} \mu(T_{n^2+m^2}^{-1} A \cap T_{m^2}^{-1} A) > 0,$$

or

$$\liminf_{N \rightarrow \infty} \mathbb{E}_{n, m \in [N]} \mu(T_{n^2+n}^{-1} A \cap T_{m^2}^{-1} A) > 0?$$

Theorem 1.6 gives criteria for the image of a Möbius transformation to be a set of topological multiplicative recurrence. However there are cases not covered by this theorem. For example, we do not know whether $\{(6n + 3)/(6n + 2) : n \in \mathbb{N}\}$ is a set of topological multiplicative recurrence. Because of this reason, we ask:

Question 7.2. For $a \in \mathbb{N}$, $b, d \in \mathbb{Z}$, is it true that $S = \{(an + b)/(an + d) : n \in \mathbb{N}\}$ is a set of topological multiplicative recurrence if and only if $a|b$ or $a|d$?

For a polynomial $P \in \mathbb{Z}[x]$, Theorem 4.3 shows that $\{P(n) : n \in \mathbb{N}\}$ contains an infinite multiplicative semigroup if and only if $P(x) = (ax + b)^d$ for some $a, d \in \mathbb{N}$, $b \in \mathbb{Z}$ with $a|b(b-1)$ and $d \in \mathbb{N}$. Here we can ask:

Question 7.3. For which polynomial $P \in \mathbb{Z}[x]$ is $\{P(n) : n \in \mathbb{N}\}$ a set of topological multiplicative recurrence?

Even the answer for the following question is unknown:

Question 7.4. Is $\{n^2 + 1 : n \in \mathbb{N}\}$ a set of topological multiplicative recurrence?

It is known that the set of shifted primes $\mathbb{P} - 1 = \{p - 1 : p \text{ is a prime}\}$ and $\mathbb{P} + 1 = \{p + 1 : p \text{ is a prime}\}$ are sets of additive recurrence. Hence it is of interest to ask:

Question 7.5. Are $\mathbb{P} - 1$ and $\mathbb{P} + 1$ sets of topological multiplicative recurrence?

We remark that neither of the sets $\mathbb{P} - 1$ and $\mathbb{P} + 1$ contain a multiplicative semigroup, since for any $a \in \mathbb{N}$ we can factor $a^2 - 1 = (a - 1)(a + 1)$ and $a^3 + 1 = (a + 1)(a^2 - a + 1)$ and hence $\mathbb{P} + 1$ does not contain a perfect square and $\mathbb{P} - 1$ does not contain a perfect cube.

REFERENCES

- [1] J. Auslander. *Minimal flows and their extensions*, volume 153 of *North-Holland Mathematics Studies*. North-Holland Publishing Co., Amsterdam, 1988. Notas de Matemática [Mathematical Notes], 122. [15](#)
- [2] V. Bergelson. Ergodic Ramsey theory—an update. In *Ergodic theory of \mathbb{Z}^d actions*, volume 228 of *London Math. Soc. Lecture Note Ser.*, pages 1–61. Cambridge Univ. Press, Cambridge, 1996. [4](#), [7](#)
- [3] V. Bergelson. The multifarious Poincaré recurrence theorem. In *Descriptive set theory and dynamical systems*, volume 277 of *London Math. Soc. Lecture Note Ser.*, pages 31–57. Cambridge Univ. Press, Cambridge, 2000. [10](#)
- [4] V. Bergelson. Multiplicatively large sets and ergodic Ramsey theory. *Israel J. Math.*, 148:23–40, 2005. [6](#), [7](#), [8](#), [9](#)
- [5] V. Bergelson. Combinatorial and diophantine applications of ergodic theory. In B. Hasselblatt and A. Katok, editors, *Handbook of Dynamical Systems*, volume 1B, pages 745–841. Elsevier, 2006. [6](#)
- [6] V. Bergelson. Questions on amenability. *Enseign. Math.*, 54(2):28–30, 2008. [10](#)
- [7] V. Bergelson and R. McCutcheon. Recurrence for semigroup actions and a non-commutative Schur theorem. In *Topological dynamics and applications (Minneapolis, MN, 1995)*, volume 215 of *Contemp. Math.*, pages 205–222. Amer. Math. Soc., Providence, RI, 1998. [8](#), [18](#)
- [8] N. Bogoliouboff and N. Kryloff. La théorie générale de la mesure dans son application à l'étude des systèmes dynamiques de la mécanique non linéaire. *Ann. of Math. (2)*, 38(1):65–113, 1937. [10](#)
- [9] P. Csikvári, K. Gyarmati, and A. Sárközy. Density and Ramsey type results on algebraic equations with restricted solution sets. *Combinatorica*, 32(4):425–449, 2012. [36](#)
- [10] P. Erdős and R. L. Graham. *Old and new problems and results in combinatorial number theory*, volume 28. Université de Genève, L'Enseignement Mathématique, Geneva, 1980. [1](#)
- [11] N. Frantzikinakis and B. Host. Higher order Fourier analysis of multiplicative functions and applications. *J. Amer. Math. Soc.*, 30(1):67–157, 2017. [1](#), [2](#), [22](#), [37](#)
- [12] H. Furstenberg. Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions. *J. d'Analyse Math.*, 31:204–256, 1977. [2](#), [4](#)
- [13] H. Furstenberg. *Recurrence in ergodic theory and combinatorial number theory*. Princeton University Press, Princeton, N.J., 1981. [8](#)
- [14] H. Furstenberg and Y. Katznelson. An ergodic Szemerédi theorem for IP-systems and combinatorial theory. *J. d'Analyse Math.*, 45:117–168, 1985. [7](#)
- [15] M. Heule, O. Kullmann, and V. Marek. *Solving and Verifying the Boolean Pythagorean Triples Problem via Cube-and-Conquer*, pages 228–245. Springer International Publishing, Cham, 2016. [1](#)
- [16] T. Kamae and M. Mendès France. Van der Corput's difference theorem. *Israel J. Math.*, 31(3-4):335–342, 1978. [4](#), [18](#)

- [17] O. Klurman and A. Mangerel. Rigidity theorems for multiplicative functions. *Mathematische Annalen*, 372:651–697, 2018. [4](#)
- [18] I. Kříž. Large independent sets in shift-invariant graphs: solution of Bergelson’s problem. *Graphs Combin.*, 3(2):145–158, 1987. [10](#)
- [19] S. Lindqvist. Partition regularity of generalised Fermat equations. *Combinatorica*, 38(6):1457–1483, 2018. [36](#)
- [20] A. Sárközy. On difference sets of sequences of integers. I. *Acta Math. Acad. Sci. Hungar.*, 31(1–2):125–149, 1978. [4](#)
- [21] W. Schmidt. *Equations over finite fields. An elementary approach*. Lecture Notes in Mathematics, Vol. 536. Springer-Verlag, Berlin-New York, 1976. [35](#)
- [22] W. Sun. A structure theorem for multiplicative functions over the Gaussian integers and applications. *J. Anal. Math.*, 134(1):55–105, 2018. [1](#)
- [23] W. Sun. Sarnak’s conjecture for nilsequences on arbitrary number fields and applications. <http://arxiv.org/abs/1902.09712>, 2019. [1](#)
- [24] T. Tao and V. Vu. *Additive Combinatorics*. Cambridge University Press, 2006. [36](#)

DEPARTAMENTO DE INGENIERÍA MATEMÁTICA AND CENTRO DE MODELAMIENTO MATEMÁTICO, CNRS IRL 2807, UNIVERSIDAD DE CHILE, BEAUCHEF 851, SANTIAGO, CHILE.

Email address: sdonos@dim.uchile.cl

DEPARTMENT OF MATHEMATICS, OHIO STATE UNIVERSITY, 231 W. 18TH AVE., COLUMBUS, OH 43210

Email address: le.286@osu.edu

MATHEMATICS INSTITUTE, UNIVERSITY OF WARWICK, COVENTRY, UK

Email address: joel.moreira@warwick.ac.uk

DEPARTMENT OF MATHEMATICS, VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY, 225 STANGER STREET, BLACKSBURG VA, 24061-1026, USA

Email address: swenbo@vt.edu