A NOTE ON FURSTENBERG'S $\times 2, \times 3$ THEOREM WITH AN ELEMENTARY AND SHORT PROOF

HAN YU

ABSTRACT. In this note we present a proof showing that the only infinite closed subset of $[0,1]$ which is invariant under $\times 2, \times 3 \mod 1$ actions is the whole interval $[0,1]$. Here we will first illustrate a proof by Furstenberg in [Fu, Part IV] and then provide a slightly different approach which leads to an elementary and short proof.

1. FURSTENBERG'S PROOF

1.1. Semi-group actions, invariant subsets, Furstenberg's Nakayama-type lemma. Let $S \subset \mathbb{N}$ be a multiplicative semi-group of integers. More precisely,

$$s_1, s_2 \in S \implies s_1 s_2 \in S.$$

For subset $A \subset [0,1]$, we call A invariant under S-action if

$$\forall s \in S, \forall a \in A, s(a) = \{sa\} \in A,$$

where $\{x\}$ is the fractional part of $x \in [0,\infty)$. For any $x \in [0,1]$, we denote the orbit $Orb_S(x) = \{s(x) : s \in S\}$ and we say that a closed S-invariant set $A \subset [0,1]$ is minimal (or S acts minimally on A) if for all $x \in A$ the orbit $Orb_S(x)$ is dense in A. Given any closed S-invariant set A, it is always possible to find (possibly more than one) $A_m \subset A$ such that A_m is minimal with respect to S (Zorn's lemma).

The S-action on $[0,1]$ turns it into a S-group (similar with modules but with semi-group action instead of ring action) in the sense that for $s_1, s_2 \in S, x_1, x_2 \in [0,1]$

$$(s_1, s_2, +)(x_1, x_2) = \{s_1 x_1 + s_2 x_2\}.$$

Notice that given any ring R and a R-module M, we can write the ring action in a similar way

$$(r_1, r_2, +)(m_1, m_2) = r_1 m_1 + r_2 m_2.$$

Now we shall focus on the multiplicative sub semi-group of $\mathbb{N}$ generated by $2, 3$. We note that results in this note hold for other semi-groups and more general phase space other than $[0,1]$ (for example the d-torus). The next result is a Nakayama-type lemma due to Furstenberg [Fu, Proposition IV.1].

Lemma 1.1. *Let M, B be two closed S-invariant subsets of $[0,1]$. If M is minimal under action S and $M + B \mod 1 = [0,1]$ then $B = [0,1]$.*

2010 *Mathematics Subject Classification.* TBD.

Key words and phrases. TBD.

Remark 1.2. *Nakayama's lemma says that for a commutative ring R with Jacobson ideal J, given any finite generated R-module N, and any submodule $M \subset N$, the following holds*

$$N = M + JM \implies M = N.$$

Proof. It is easy to check that $2, 3$ are primitive roots modulo 5. More precisely, for $k = 0, 1, 2, 3, \ldots$

$$2^k \equiv 1, 2, 4, 3, 1, 2, 4, 3 \ldots \mod 5.$$

Similar result holds for $3^k, k \in \mathbb{N}$ as well. Some further number theoretic argument can deduce that $2, 3$ are primitive roots modulo 5^K for all integer $K \geq 1$($(\mathbb{Z}/5^K\mathbb{Z})^*$ is cyclic). Now we consider rational numbers with denominator $5^K, K \in \mathbb{N}$ (or 5-adic numbers). More precisely we consider the following set

$$A_5(K) = \{a5^{-K} : \exists a \in [0, 5^K] \cap \mathbb{N}\}.$$

Notice that if m is an integer such that $m \equiv 1 \mod 5^K$, then $\times m \mod 1$ acts as the identity on $A_5(K)$. Now let us consider the sub action of S defined as follows

$$S(K) = \{s \in S : s \equiv 1 \mod 5^K\}.$$

Then we see that $S(K)$ is an infinite sub semi-group of S. Indeed, for any $s \in S$ there exist infinitely many integer n such that

$$s^n \equiv 1 \mod 5^K.$$

Now we can find a closed subset of M which is minimal under action $S(K)$ and denote it as $M(K)$. We want to show that $M(K)$ is not too small. Now define the following 'cosets' of $S(K)$

$$S(K, r) = \{s \in S : s \equiv r \mod 5^K\}, r \in \{1, 2, \ldots, 5^K - 1\}.$$

Clearly, we only need to consider r to be one of the residues of S modulo 5^K. We write the residue set as S_{5^K}. For each of those residue r we can find a smallest integer $s(r) \in S$ such that $s(r) \equiv r \mod 5^K$. As a result we see that $s(r)M(K)$ is minimal under $S(K)$. We write now the following set

$$M' = \bigcup_{r \in S_{5^K}} s(r)M(K).$$

Clearly M' is closed and it is a finite union of minimal sets. Let $s \in S$ and $r \in S_{5^K}$ and we consider $ss(r)M(K)$. Suppose that $s \equiv t \mod 5^K$ and then $ss(r) \equiv tr \mod 5^K$. Therefore $ss(r) \in S(K, rt)$. Let $s(rt)^l \equiv 1 \mod 5^K$, then $ss(r)s^l(rt) \in ss(r)S(K)$ and $ss(r)s^{l-1}(rt) \in S(K)$. Then as $M(K)$ is $S(K)$ invariant we see that

$$ss(r)s(rt)s^{l-1}(rt)M(K) \subset s(rt)M(K).$$

In particular we have found $x \in ss(r)M(K) \cap s(rt)M(K)$ and because of the minimality of $ss(r)M(K), s(st)M(K)$ under $S(K)$ we see that

$$ss(r)M(K) = s(st)M(K).$$

Indeed, we only need to consider $Orb_{S(K)}(x)$ and it is dense in $ss(r)M(K)$ as well as $s(st)M(K)$. This implies that M' is invariant under S action and because $M' \subset M$ and M is minimal under S we see that $M' = M$.

Since $M + B = [0, 1]$ and $M = \bigcup_{r \in S_{5^K}} s(r)M(K)$ we see that at least one of $s(r)M(K)$ is such that $s(r)M(K) + B$ has positive Lebesgue measure. Notice that $s(r)M(K) + B$ is invariant under $S(K)$-action and in particular invariant under the $\times m \mod 1$ action for any integer $m \in S(K)$ and therefore $s(r)M(K) + B$ has full Lebesgue measure and because it is closed we see that $s(r)M(K) + B = [0, 1]$. This means that for all $x \in [0, 1]$ we can find $a \in s(r)M(K), b \in B$ such that $a + b \mod 1 = x$. Now we choose $x \in A_5(K)$ and apply $S(K)$-action on the equation

$$a + b = x \mod 1$$

Now fix any $a_0 \in s(r)M(K)$. Since $S(K)$ acts as identity on $A_5(K)$ and minimally on $s(r)M(K)$ we can find a sequence $s_i \in S(K), i \in \mathbb{N}$ such that

$$s_i(a) \to a_0, s_i(b) \to b' \in B, s_i(x) \to x.$$

Notice that the equality $s(a)+s(b) = s(x) = x \mod 1$ holds for all $s \in S(K)$ and we see that

$$a_0 + b' = x.$$

This implies that $a_0 + B$ is 5^{-K}-dense in $[0, 1]$. Then because K can be chose arbitrarily we see that B is dense in $[0, 1]$. Since B is closed we see that $B = [0, 1]$. $\square$

1.2. **irrational rotation and closed $\times 2, \times 3$ invariant sets.**

Lemma 1.3. *Let $A \subset [0, 1]$ be a closed S-invariant set where S is the multiplicative semi-group generated by $\{2, 3\}$. If $0 \in A$ is not isolated then $A = [0, 1]$.*

Proof. Consider intervals $I_k = [0, 3^{-k}], k \in \mathbb{N}$. Since $0 \in A$ is not isolated we can find infinitely many $k \in \mathbb{N}$ and $a_k \in A$ such that

$$a_k \in I_k \setminus I_{k+1}.$$

Then $2^{k_1}3^{k_2}a_k \in A$ for all k_1, k_2 such that $2^{k_1}3^{k_2} \leq 3^{k+1}$. By taking logarithm we see that

$$k_1 \log 2 + k_2 \log 3 + \log a_k \in \log(A \setminus \{0\}).$$

Or equivalently we have for all k_1, k_3 with $k_1 \log 2 - k_3 \log 3 \leq \log 3$

$$\log 3^k a_k + k_1 \log 2 - k_3 \log 3 \in \log(A \setminus \{0\}).$$

Now we can choose integers k_1, k_3 in a dynamical way. Let $k_1(0) = 0, k_3(0) = 0$ be our initial state. We define now the following map

$$T(x, y) = \begin{cases} (x + 1, y), \text{ if } (x + 1) \log 2 - y \log 3 \leq \log 3 \\ (x + 1, y + 1), \text{ if } (x + 1) \log 2 - y \log 3 > \log 3. \end{cases}$$

Now we choose $(k_1(i), k_3(i)) = T^i(0, 0)$ for integers $i \leq \lfloor k \frac{\log 3}{\log 2} \rfloor$. Then we see that $k_1(i), k_3(i)$ satisfy the condition $2^{k_1(i)}3^{k_2(i)} \leq 3^{k+1}$ for $k_2(i) = k - k_3(i)$ and $k_2(i) \geq 0$. Then we see that

$$\alpha(i) = k_1(i) \log 2 - k_3(i) \log 3 = \{i \log 2/ \log 3\} \log 3.$$

As $\log 2/ \log 3$ is irrational we see that if k is large enough $\alpha(i), i \leq \lfloor k \frac{\log 3}{\log 2} \rfloor$ will be eventually dense enough. More precisely, for any $\epsilon > 0$ there is a $N(\epsilon) > 0$ such that $\alpha(i), i \leq N(\epsilon)$ is ϵ-dense in $[0, \log 3]$. Now choose a

k such that $k \geq N(\epsilon)$ we see that for k_1, k_2 running over all choices with $2^{k_1}3^{k_2} \leq 3^{k+1}$ the following set

$$\{\log(2^{k_1}3^{k_3}a_k)\}_{k_1,k_2 \text{ as stated above}}$$

is ϵ dense in $\log 3^k a_k + [0, \log 3]$. Now notice that $3^k a_k \in [1/3, 1]$ and $\exp(.)$ is smooth on $[1/3, 1]$, we see that there is $\delta(\epsilon) = O(\epsilon)$ such that

$$\exp\{\log(2^{k_1}3^{k_3}a_k)\}_{k_1,k_2 \text{ as stated above}}$$

is $\delta(\epsilon)$-dense in $[1, 3]$. Here $\delta(\epsilon) = 100\epsilon$ is a valid choice. Then after performing the $\mod 1$ operation we see that A is 100ϵ-dense in $[0, 1]$, then because $\epsilon > 0$ can be chosen arbitrarily we see that A is dense and therefore equal to $[0, 1]$ because A is closed. □

Now we can finally conclude the following result.

Theorem 1.4. *Let $A \subset [0, 1]$ be a closed S-invariant set where S is the multiplicative semi-group generated by $\{2, 3\}$. If A is infinite then $A = [0, 1]$.*

Proof. Since A is infinite we see that $A - A$ is a closed S-invariant set and $0 \in A - A$ is not isolated. Then we see that $A - A = [0, 1]$. If we assume that A is minimal under S then by Lemma 1.1, $A = [0, 1]$. If A is not minimal, we conclude that any minimal subset A_m of A is either $[0, 1]$ or else $A_m - A_m$ does not contain 0 as a non-isolated point. In the later case A_m must be finite. Then it is easy to see that A_m cannot contain irrational numbers. In the former case $A_m = [0, 1]$, but this is certainly not a minimal set under S because $1/2 \in A_m$ and $Orb_S(1/2) = \{0, 1/2, 1\}$ is a proper closed subset invariant under action S. We conclude that all minimal subsets of A are finite and consist only rational numbers.

If A contains only rational numbers then $A - A$ can not be $[0, 1]$ and therefore A is finite. If A contains an irrational number $\zeta \in (0, 1)$, then we consider the orbit $Orb_S(\zeta)$ which consists only irrational numbers. However $A_\zeta = \overline{Orb_S(\zeta)}$ is closed and S-invariant therefore it contains a minimal subset $A' \subset A_\zeta$. Then we see that A' consists finitely many rational numbers. Therefore A_ζ contains a rational number p/q. Then qA_ζ contains 0 as a non-isolated point, thus $qA_\zeta \mod 1 = [0.1]$. This implies that $qA \mod 1 = [0, 1]$. Thus A has positive Lebesgue measure and therefore full Lebesgue measure and therefore $A = [0, 1]$. □

2. A SLIGHTLY DIFFERENT PROOF

We now provide a different proof without using Lemma 1.1. We will borrow the (elementary) argument in the proof of Lemma 1.3. From there, (just as the first step in the proof of Theorem 1.4) we could easily conclude that $A - A = [0, 1]$. From here, our argument differs slightly.

Without loss of generality, we assume that A is the orbit closure of S with an irrational stating point. This implies that A cannot contain isolated rational points.

Take an integer $l \geq 10$. Take $a \in A$ such that there is $b \in A$ with $a - b = 5^{-l}$. Such pairs exist as we just showed. Now take integers k_1, k_2 such that $2^{k_1} \equiv 3^{k_2} \equiv 1 \mod 5^l$ (cyclicity of the multiplicative group of units in $\mathbb{Z}/5^l\mathbb{Z}$). Then take S' to be the semi-group generated by $2^{k_1}, 3^{k_2}$. For each

$s \in S'$, $s(a) - s(b) = 5^{-l}$. From here we conclude that for each $x \in \overline{Orb_{S'}(a)}$, there is a point $y \in A$ with $x - y = 5^{-l}$. We want to take an irrational point in $\overline{Orb_{S'}(a)}$. This is possible as long as we can choose a to be irrational. If a is rational, then it is not isolated in A. This in turn implies that $A = [0,1]$. So without loss of generality, we can assume that a is irrational. By using the argument in the proof of Lemma 1.3 again for times $2^{k_1}, 3^{k_2}$ actions, we conclude that $\overline{Orb_{S'}(a)} - \overline{Orb_{S'}(a)} = [0,1]$. We can then find a point $a' \in \overline{Orb_{S'}(a)}$ with points $b', b'' \in \overline{Orb_{S'}(a)}$ such that

$$a' - b' = 5^{-l}, a' - b'' = 2 \times 5^{-l}.$$

We can take a' to be irrational, otherwise, if a' is rational, then it is not isolated (in $\overline{Orb_{S'}(a)} \subset A$) and we conclude that $A = [0,1]$. We then perform the above argument one more time to obtain point a'' in A with the property that $a'' + k5^{-l} \in A$ for $k = 0, 1, 2$. If the above argument can be performed indefinitely for infinitely many $l \geq 10$, we then find in A, 5^{-l}-dense subsets of $[0,1]$. This implies that $A = [0,1]$. If the above argument cannot be performed as in above, then we can find a rational non-isolated point in A and this forces $A = [0,1]$. From here the proof finishes.

REFERENCES

[Fu] H. Furstenberg *Disjointness in Ergodic Theory, Minimal Sets, and a Problem in Diophantine Approximation*, MATHEMATICAL SYSTEMS THEORY, Vol. I, No. 1.

HAN YU, SCHOOL OF MATHEMATICS & STATISTICS, UNIVERSITY OF ST ANDREWS, ST ANDREWS, KY16 9SS, UK,

E-mail address: hy25@st-andrews.ac.uk