A FRACTAL POINT OF VIEW TOWARDS SZEMERÉDI'S THEOREM

HAN YU

Abstract. The motivation of this paper is to link Szemerédi 's theorem with fractal dimensions with a hope to gain some new point of view towards Szemerédi 's theorem. We show here that the Szemerédi 's theorem is equivalent to a F_σ sub-semi group having Hausdorff dimension less than 1. An important ingredient here is a result by Lindenstrauss, Meiri and Peres on convolution of S^1 measures.

1. Introduction

In this paper, we make a simple observation that links Szemerédi 's theorem to fractal dimensions. The object we study in this paper is the set of numbers in $[0,1]$ whose binary digit expansion does not have arbitrarily long arithmetic progressions of positions of digit 1. Such set will be defined and discussed in section 5.

On one hand, Szemerédi 's theorem tells us that the Hausdorff dimension of the above set is 0. On the other hand, without the knowledge of Szemerédi 's theorem, we can show that the Hausdorff dimension of the above set is either 0 or 1, and if one can show that the Hausdorff dimension of not equal to one then another proof of Szemerédi 's theorem can be found.

The Szemerédi 's theorem of arithmetic progressions is perhaps one of the most active part of mathematics in recent decades. There is no lacking of materials of this topic. For original references see [Sze75], [FKO82], [Gow01].

2. Densities and dimension

In this section we introduce the notion of densities and dimensions that will be used in this paper.

For now consider $A \subset \mathbb{N}$ be a sequence of integers and denote

$$A(n) = \#|i \in [1,n] : i \in A|.$$

Definition 2.1. *The upper/lower natural density of A is defined as*

$$\limsup_{n\to\infty} / \liminf_{n\to\infty} \frac{A(n)}{n}.$$

Definition 2.2. *The upper Banach density of A is defined as*

$$\limsup_{k,M\to\infty} \frac{1}{k}(A(M+k-1) - A(M)).$$

2010 *Mathematics Subject Classification.* Primary: 11B25, 37A45 Secondary: 28A80.
Key words and phrases. Hausdorff dimension, sum sets, Szemerédi 's theorem.

The upper/lower natural density have their fractal dimension counterpart as upper/lower box dimension. The lower box dimension can often be replaced by Hausdorff dimension. The upper Banach density can be considered as the Assouad dimension.

In this paper we will mostly work with Hausdorff dimension therefore we will only put the definition of Hausdorff dimension here. For other notions of dimensions see [Fal04], [Mat99]. For arithmetic progressions in a different setting see [FH17], [FKH17].

Consider now $A \subset [0,1]$ to be a Borel set.

For any $s \in \mathbb{R}^+$ and any $\delta > 0$ define the following quantity:

$$\mathcal{H}^s_\delta(A) = \inf\left\{\sum_{i=1}^{\infty}(\mathrm{diam}U_i)^s : \bigcup_i U_i \supset A, \mathrm{U_i} < \delta\right\}.$$

Then the s-Hausdorff measure of A is:

$$\mathcal{H}^s(A) = \lim_{\delta \to 0} \mathcal{H}^s_\delta(A).$$

The Hausdorff dimension of A is:

$$\dim_{\mathrm{H}} A = \inf\{s \geq 0 : \mathcal{H}^s(A) = 0\} = \sup\{s \geq 0 : \mathcal{H}^s(A) = \infty\}.$$

3. Hausdorff dimension and convolution of measures

A important ingredient is a result in [LMP99]. In fact we will only need the following weak result.

Theorem 3.1. *Let $E \subset [0,1]$ be a $\times p \mod 1$ invariant closed set, then if* $\dim_{\mathrm{H}} E > 0$

$$\dim_{\mathrm{H}}(E + \cdots + E) \to 1.$$

Denote $T : [0,1] \to [0,1]$ by $T(x) = px \mod 1$, then a T invariant set $E \subset [0,1]$ satisfies $TE \subset E$.

In particular if $E + \cdots + E \subset E_\infty$ for a Borel subset E_∞ of $[0,1]$ then

$$\dim_{\mathrm{H}} E_\infty = 1.$$

The second important ingredient is the van der Waerden's theorem [vdW27]. Which says that for any finite decomposition of integers, there is a component of the decomposition with arbitrarily long arithmetic progressions.

Another ingredient is the following simple observation:

Lemma 3.2. *Let $S = s_1 s_2 \dots$ be a $0,1$ sequence whose digit 1 has lower natural density $\alpha > 0$. Then define the following set*

$$E_S = \left\{x \in [0,1] : x = \sum_{i=1}^{\infty} x_i 2^{-i}, x_i \in \{0,1\} \text{ if } s_i = 1 \text{ and } x_i = 0 \text{ if } s_i = 0\right\}.$$

Then

$$\dim_{\mathrm{H}} E_S \geq \alpha.$$

Proof. We can define a 1/2-Bernoulli measure supported on E_S in a standard manner. More precisely define

$$\mu = \star_{i=1}^{\infty}\left(s_i\left(\frac{1}{2}\delta_{1/2} + \frac{1}{2}\delta_0\right) + (1 - s_i)\delta_0\right)$$

Here δ_x is the Dirac measure supported on point $x \in [0,1]$. By construction we see that $\mu(E_S) = 1$.

Let I be a dyadic interval of length 2^{-N} for a large integer N such that

$$\#|i \in [1,N] : s_i \neq 0| \geq 0.9\alpha N.$$

The above inequality holds for all large enough N by the definition of lower natural density.

Then

$$\mu(I) \leq \left(\frac{1}{2}\right)^{\#|i\in[1,N]:s_i\neq 0|} \leq \left(\frac{1}{2}\right)^{0.9\alpha N}.$$

Therefore for all dyadic interval I:

$$\mu(I) \leq |I|^{0.9\alpha}.$$

This implies that μ is a regular (Frostman) measure, this implies that

$$\dim_{\mathrm{H}} E_S \geq 0.9\alpha.$$

Here 0.9 can be replaced by any number smaller than 1 and this lemma concludes. □

4. Simple reductions of Szemerédi 's theorem

In this section we reduce the Szemerédi 's theorem for upper Banach density to lower natural density and in a fractal geometry point of view our approach is the following:

$$\text{Assouad dimension} \implies \text{box dimension} \implies \text{Hausdorff dimension}$$

We take the upper Banach density version of Szemerédi 's theorem, that for any sequence with positive upper Banach density one can find arbitrarily long arithmetic progressions.

For the reader who is satisfied with the lower natural density version, this section can be skipped.

This is likely to be known but it is nice to be included here for later development.

Lemma 4.1. *If any sequence with positive upper natural density consists arbitrarily long arithmetic progression, then the same holds if we only require the sequence to have positive upper Banach density.*

Remark 4.2. *In fact for any sequence with upper Banach density $\alpha > 0$ we shall construct a sequence with upper natural density arbitrarily close to α. If the new sequence contains arbitrarily long progression then the original one has the same property.*

Proof. Let $0 < \rho < 1, M > 1$ be any real numbers which can be chosen arbitrarily. Let $A \subset \mathbb{N}$ such that the upper Banach density is $\alpha > 0$. From the definition of upper Banach density we see that there is a sequence of integers $N_i \to \infty$ such that for any i, there exist an integer k_i such that:

$$\#|A \cap [k_i, k_i + N_i - 1]| \geq \rho\alpha N_i.$$

By taking a further subsequence if necessary we can assume that $N_{i+1} > MN_i$ for all i. Define a sequence w_i by:

$$w_i = \sum_{s=1}^{i} N_s.$$

Now we want to manipulate the original sequence A. Let $A_i = A\cap[k_i, k_i+N_i-1]$. Define a new sequence $B\subset\mathbb{N}$ by the following

$$B=\bigcup_i (A_i-k_i+w_i).$$

This sequence B is constructed by shifting each A_i into the interval $[w_i, w_i+N_i-1]$. The upper natural density of B is bounded from below by:

$$\overline{d}B \geq \limsup_i \frac{\#|A_i|}{\sum_{s=1}^{i} N_i} \geq \limsup_i \rho\frac{\alpha N_i}{N_i\sum_{s=1}^{i} M^{-s+1}} \geq \frac{\rho M}{M-1}\alpha > 0.$$

By assumption, B contains arbitrarily long arithmetic progression. We want to show that the progressions mainly lay in intervals $[w_i, w_i+N_i-1]$.

Suppose there is a k-term progression P inside B, where $k\geq 4$ is an integer. Then suppose the first term of P is in $A_i-k_i+w_i$ for some integer i.

Suppose the second term is also in this interval and the progressions spans over Q intervals and terminate at the $Q+1$-th interval. Then we see that because the length of the intervals grows at least exponentially and the gap of progression is smaller than N_i:

$$M+M^2+\cdots+M^Q\leq k.$$

This implies that:

$$Q\leq\frac{\log(k+1)}{\log M}.$$

Then in at least one of the intervals the progression has no less than:

$$k/Q\geq\frac{k}{\log(k+1)}\log M$$

terms. If this holds for arbitrarily large k then the original sequence also contains arbitrarily long progressions.

Similarly if the second term is in another interval say $A_{i+m}-k_{i+m}+\omega_{i+m}$. Then the gap is bounded by $N_{i+m}(1+M^{-1}+\cdots+M^{-m})\leq N_{i+m}\frac{M}{M-1}$. Then we can argue in the same as before suppose the sequence span Q intervals and stop at the $Q+1$-the one (with a loss of factor $\frac{M-1}{M}$ but this is ignorable if M is large):

$$\frac{M-1}{M}(M+M^2+\cdots+M^Q)\leq k.$$

Then again we see that at least in one interval the progression has no less than:

$$\frac{k}{\log(k+1)}\log M$$

terms.

By choosing ρ, M properly the upper density of the new sequence can be arbitrarily close to the original one. □

With the same argument we can reduce the case to lower natural density as well.

Lemma 4.3. *If any sequence with positive lower natural density consists arbitrarily long arithmetic progression, then the same holds if we only require the seqence to have upper natural density.*

Remark 4.4. *In fact for any sequence with upper natural density $c > 0$ we shall construct a sequence with lower natural density arbitrarily close to $c/3$ (careful analysis can give us $c/2$ it would be interesting if one can get c). If the new sequence contains arbitrarily long progression then the original one has the same property.*

Proof. Let $0 < \rho < 1$ be a real numbers Assume A has upper natural density $c > 0$, then we can find a number $N_1 > 0$ such that:

$$\#|A \cap [1, N_1]| \geq \rho c N_1.$$

Then we call interval $A \cap [1, N_1]$ as I_1.

Then we can find a $N_2 > 2N_1$ such that $\#|A \cap [N_1+1, N_1+N_2+1]| \geq \rho c(N_2 - N_1)$. Then there is at least one interval of length equal to $2N_1$ and the density of A on this interval is at least ρc. We now relabel $N_2 = 2N_1$ and call this interval I_2.

Then we can go on finding intervals I_k such that the length of I_k is 2 times that of I_{k-1} and densities on each interval are bounded below by ρc.

Now we construct a new sequence B connecting I_k together. Namely,

$$B_i = A_i, i \in \{1, N_1\}.$$

Then we put a copy of I_2

$$B_i = A_i, i \in \{N_1 + 1, N_1 + N_2 + 1\}.$$

And the rest can be done inductively.

Now we see that:

$$\frac{\#|B \cap [1, N]|}{N}$$

when N are in the k-th translated interval I_k changes between:

$$c\rho \text{ and } c\rho/3$$

So B has positive lower natural density at least ρc therefore contains arbitrarily long arithmetic progressions. Then similar argument as in previous lemma leads us the conclusion. □

5. The fractal setting up

In this section we translate the combinatorial problem concerning arithmetic progressions into dimension problem of subset of unit intervals.

Let $x = x_1 x_2 \dots$ be a $0, 1$ sequence. Then we denote x to be the following real number as well:

$$x = \sum_{i=1}^{\infty} 2^{-i} x_i.$$

Such association is not one-one, however, the only two to one situations happen when the real number x is a dyadic rational. In this case, we shall assume the sequence x to have only finitely many 1's. That is, we will not consider the sequence with only finitely many 0's. We will use this identification of $0, 1$ sequences with real numbers in $[0, 1]$.

For any two real numbers $x, y \in [0, 1]$ which are not dyadic rational , we say x is a subsequence of y if in binary expansion we have the following relation:

$$\forall i \geq 1, x_i = 1 \implies y_i = 1.$$

We shall also use intersection/union of two real numbers $x, y \in [0, 1]$ to denote their bitwise AND/OR operations.

Precisely, z is the intersection resp. union of x and y in $[0,1]$ if for all $i \geq 1$, $z_i = x_i y_i$ resp. $z_i = 1-(1-x_i)(1-y_i)$.

Lemma 5.1. *Let x, y be two sequences (real numbers in $[0,1]$), such that the positions of 1's in each sequence do not contain arbitrarily long arithmetic progressions. Then $x+y \mod 1$ has the same property, namely, binary expansion of $x+y \mod 1$ does not contain arbitrarily long arithmetic progressions either.*

Remark 5.2. *The maximal length of arithmetic progressions which are contained in $x+y \mod 1$ is in general larger than that of x and y.*

Proof. Let sequences x, y be free of k-term progressions. Then we can perform the sum $x+y$ in several steps:

1 : Define two sequences s, r of $0,1$ by $i \geq 1$:

$$\begin{aligned} s_i &= 1 && \text{if precisely one of } x_i, y_i \text{ is equal to 1,} \\ s_i &= 0 && \text{otherwise.} \\ r_i &= 1 && \text{if both } x_{i+1}, y_{i+1} \text{ are 1,} \\ r_i &= 0 && \text{otherwise.} \end{aligned}$$

It is clear that $x+y = s+r \mod 1$.

2 : Define two sequences s', r' of $0,1$ by $i \geq 1$:

$$\begin{aligned} s'_i &= s_i + r_i && \text{if precisely one of } s_i, r_i \text{ is equal to 1,} \\ s'_i &= s_i && \text{otherwise.} \\ r'_i &= 0 && \text{if } s_i = 0, r_i = 1, \\ r'_i &= r_i && \text{otherwise.} \end{aligned}$$

It is clear that $x+y = s'+r' \mod 1$.

3 : After the above two steps, we see that s' is a $0,1$ sequence. Then s' is a concatenation of blocks of $0's$ and $1's$. Between two successive blocks of $1's$, there is at least one 0 digit. When $s'_i = 0$ we see that $r'_i = 0$ as well. The last step is to perform $s'+r'$ for individual blocks of $1's$. It is easy to see that for each individual block, the sum of s', r' will not disturb other blocks of $1's$. Because the sum will change at most one digit 0 next to the leftmost of a block of $1's$. For example:

$$\dots 0111110 \dots + \dots 0001010 \dots = \dots 1001000 \dots$$

Let us now examine arithmetic progressions in each step. After step 1, both r, s do not contain arbitrarily long arithmetic progressions. For r this is easy to see because r is essentially a shifted version of a subsequence of x. For s, it is a subsequence of the union of sequences x, y. If s contains arbitrarily long arithmetic progressions, then by van der Waerden's theorem one of x, y must contain arbitrarily long arithmetic progressions as well. Similar argument holds for step 2 as well.

For the last step, if $x+y \mod 1$ contains arbitrarily long progressions, then there is arbitrarily long progressions on digits of $1's$ of one of the following types:

1. the digit 1 is an unchanged 1 from s'.
2. the digit 1 is a digit 1 of the same position in r'.
3. the digit 1 is a new 1 resulting from step 3 by performing the sum. This digit is next to the leftmost position of blocks of $1's$ of s'.

Arbitrarily long progressions of each of the above type will result arbitrarily long progressions in either x or y and this is a contradiction. □

Definition 5.3. *We say $x \in [0,1]$ is Erdősian, if x is not a dyadic rational and the binary expansion of x does not contain arbitrarily long arithmetic progressions of positions of digit* 1.

The collection of all Erdősian numbers is a subset of $[0,1]$, *we call it the Erdős set* E.

Lemma 5.4. *The Erdős set E is a F_σ set.*

Proof. We do not need to consider dyadic rational numbers, as there are only countably many of them.

We can write E as a countable union in the following way:

$$E = \bigcup_{i \geq 3} E_i,$$

where $E_i, i \geq 3$ are subsets of $[0,1]$ defined as follows:

$x \in E_i \iff x$ is not a dyadic rational and the binary expansion of x does not contain any i-term arithmetic progressions of positions of digit 1.

Lets consider a sequence $\{x_k\}_{k \in \mathbb{N}} \subset E_i$. Suppose that

$$x_k \to x \in [0,1].$$

Assume that x has a i-term arithmetic progression of position of digit 1 in its binary expansion. Suppose the last term of such progression is the n-th digit. Then if k is large enough we see that $|x_k - x| \leq 2^{-n}$ and x_k would also contain a i-term arithmetic progression. This is not possible therefore we see that $x \in E_i$ as well provided that x is not a dyadic rational number. However if x is a dyadic rational number then its binary expansion certainly contains long progressions of positions of digit 1, in fact a infinite long progression, then the above argument gives us a contradiction again.

This implies that E is a F_σ set. □

Let us now take a close look at the set E_i appeared in the above proof:

Definition 5.5. *For each integer $i \geq 3$ define the following closed set $E_i \subset [0,1]$: $x \in E_i \iff x \in [0,1]$ is not a dyadic rational number and the binary expansion of x does not contain any i-term arithmetic progressions of positions of digit* 1.

Theorem 5.6. *The Erdős set E is sum stable:*

$$E \supset E + E \mod 1.$$

Proof. This is a direct conclusion of lemma 5.1. □

Corollary 5.7. *For any integer $i \geq 3$ and $N \geq 2$:*

$$\sum_{k=1}^{N} E_i \subset E.$$

6. Relation with Szemerédi's theorem

We know that the Erdős set E is Borel and sum stable, from here it is immediate that the Fourier dimension of E must be 0. This is not a new result, in fact Szemerédi 's theorem implies that E has Hausdorff dimension 0. However we note that the fact that Fourier dimension of E is 0 can be proved without the knowledge of Szemerédi 's theorem.

Theorem 6.1. *Szemerédi 's theorem* $\implies \dim_{\mathrm{H}} E = 0$.

Proof. We have the decomposition $E = \bigcup_{i\geq 3} E_i$ which was mentioned before. Now each E_i is closed and have lower box dimension 0. To see the reason, for a large integer N, there are not so many $0,1$ sequences which do not contain i-term arithmetic progressions. In fact let $\epsilon > 0$ be a small positive number. Let N be a large integer and we can count the number of $0,1$ sequences of length N with less than ϵN many digit 1. By Chernoff-Hoeffding inequality [Hoe63], this number is

$$O(\exp(-D(\epsilon)N)2^N)$$

here

$$D(\epsilon) = \epsilon \log 2\epsilon + (1-\epsilon)\log 2(1-\epsilon) = \log 2 + \epsilon\log\epsilon + (1-\epsilon)\log(1-\epsilon).$$

Therefore the $O(.)$ is now

$$O(0.5^{\epsilon\log\epsilon + (1-\epsilon)\log(1-\epsilon)}).$$

If ϵ is small enough, the above gives box dimension 0.

From here the result follows because then $\dim_{\mathrm{H}} E_i = 0$ and Hausdorff dimension is countable union stable. □

On the other hand, it is not hard to see that:

$$\dim_{\mathrm{H}} E = 0 \implies \text{Szemerédi 's theorem}.$$

Indeed, if Szemerédi 's theorem would be not true, then we can find a sequence of integers of positive upper Banach density without containing arbitrarily long arithmetic progressions. Then by the discussions in section 4 we can assume this sequence has positive natural lower density. Then lemma 3.2 gives us the conclusion that $\dim_{\mathrm{H}} E > 0$.

We shall show the following result without the knowledge of the Szemerédi 's theorem

Theorem 6.2.

$$\dim_{\mathrm{H}} E \in \{0, 1\}.$$

Remark 6.3. *We can compare this result with another result in* [EV66] *which says that there exist Borel subgroup of* S^1 *with any Hausdorff dimension in between* 0 *and* 1*.*

Proof. Suppose that $\dim_{\mathrm{H}} E > 0$ as $E = \bigcup_{i\geq 3} E_i$ there is at least one $i \geq 3$ such that $\dim_{\mathrm{H}} E_i > 0$.

As E_i is closed and $\times 2 \mod 1$ invariant, by theorem 3.1

$$\dim_{\mathrm{H}}(E_i + \cdots + E_i) \to 1.$$

We have also the following

$$E_i + \cdots + E_i \subset E,$$

so $\dim_{\mathrm{H}} E = 1$. This concludes this theorem.

□

So we have the following logic loop

$$\text{Szemerédi 's theorem} \iff \dim_{\mathrm{H}} E = 0 \implies \dim_{\mathrm{H}} E \neq 1 \implies \dim_{\mathrm{H}} E = 0.$$

7. Further comments, ideas and hopes

Some possible further developments are listed here, the main motivation is to find a 'fractal' proof of Szemerédi 's theorem. Everything is reduced to show that $\dim_{\mathrm{H}} E \neq 1$.

Spectral gap

The set E is an countable union of closed $\times 2 \mod 1$ invariant sets and it is itself sum stable, however we can not say anything more than the spectral gap property of the Hausdorff dimension of this set.

One hope is to show that any countable union of closed $\times 2 \mod 1$ invariant sets which is sum stable and not itself the whole interval must have Hausdorff dimension smaller than 1.

Projection

What happens if $\dim_{\mathrm{H}} E = 1$, we see that for Lebesgue almost every point $a \in [0, 1]$

$$E + aE$$

has positive measure. Use the sum stability of E, we see that $E + aE$ contains intervals. So if one can show that $E + aE$ can not contain intervals then the Szemerédi 's theorem follows.

Mixing two integer bases

We can construct binary Erdős set and ternary Erdős set. They are both F_σ and ternary Erdős set is a union of closed $\times 3 \mod 1$ invariants.

We write $E^2 = \bigcup_{i\geq 3} E_i^2$ and $E^3 = \bigcup_{i\geq 3} E_i^3$.

E_i^2 are just the sets defined in previous section. E^3 can be defined similarly, more precisely:

For each integer $i \geq 3$ define the following closed set $E_i^3 \subset [0, 1]$: $x \in E_i \iff x \in [0, 1]$ is not a 3-adic rational number and the ternary expansion of x does not contain any i-term arithmetic progressions of positions of non zero digits.

Then $E_i^2 \times E_j^3$ for any pair i, j has interesting properties. For example the Hausdorff dimension of projection hit the maximum value apart from the two coordinate projections. For example if $\dim_{\mathrm{H}} E^2 = \dim_{\mathrm{H}} E^3 = 1$ then we can find i, j such that

$$\dim_{\mathrm{H}} E_i^2 + \dim_{\mathrm{H}} E_j^3 > 1.$$

This implies that $\dim_{\mathrm{H}}(E_i^2 + E_j^3) = 1$.

Changing integer bases

By Chernoff-Hoeffding inequality we see that there exist $x \in E$ such that in the binary expansion of x, the digit 1 has lower natural density at least $1/3$ (or something arbitrarily close to $1/2$).

The binary setting can be generalized to any integral base. We can the focus on positions of non zero digits. As there are only finitely many of them, we can use van der Waerden's theorem.

Now we can make the following statement (the number 0.999 can be replaced by anything smaller than 1).

Statement 7.1. *If any sequence of lower natural density* 0.999 *contains arbitrarily long arithmetic progressions then it is enough to require for positive lower natural density.*

On the other hand it is easy to show that any sequence of natural density equal to 1 must contain arbitrarily long consecutive elements.

Unfortunately, all the proofs of the Szemerédi 's theorem rely on the density increment argument which does not depends on the density of the sequence we start with. The above statement is at least morally easier to prove than the Szemerédi theorem in its full generality.

8. Acknowledgement

This manuscript was written when the author was visiting Institut Mittag-Leffler during the program 'fractal geometry and dynamics'.

References

[EV66] P. Erdös and B. Volkmann, *Additive gruppen mit vorgegebener hausdorffscher dimension*, Journal für Die Reine und Angewandte Mathematik **221** (1966), 203–208.

[Fal04] K. Falconer, *Fractal geometry: Mathematical foundations and applications*, Wiley, 2004.

[FH17] J. Fraser and H.Yu, *Arithmetic patches, weak tangents, and dimension*, Bulletin of the London Mathematical Society (2017).

[FKH17] J. Fraser, K.Saito, and H.Yu, *Dimensions of sets which uniformly avoid arithmetic progressions*, International Mathematics Research Notices (2017), rnx261.

[FKO82] H. Furstenberg, Y. Katznelson, and D. Ornstein, *The ergodic theoretical proof of szemeredi's theorem*, Bulletin of the American Mathematical Society **7** (1982), 527–552.

[Gow01] W. T. Gowers, *A new proof of szemeredi's theorem*, Geometric and Functional Analysis GAFA **11** (2001), 465–588.

[Hoe63] W. Hoeffding, *Probability inequalities for sums of bounded random variables*, Journal of the American Statistical Association **58** (1963), no. 301, 13–30.

[LMP99] E. Lindenstrauss, D. Meiri, and Y. Peres, *Entropy of convolutions on the circle*, Annals of Mathematics **149** (1999), no. 3, 871–904.

[Mat99] P. Mattila, *Geometry of sets and measures in euclidean spaces: Fractals and rectifiability*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, 1999.

[Sze75] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression.*, Acta Arith. **27** (1975), 199–245 (English).

[vdW27] van der Waerden, *Beweis einer baudetschen vermutung*, Nieuw Arch. Wisk (1927), 212–216.

Han Yu, School of Mathematics & Statistics, University of St Andrews, St Andrews, KY16 9SS, UK,

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