Miklós Laczkovich,* Department of Analysis, Eötvös Loránd University, Múzeum krt. 6-8, Budapest, H-1088 Hungary

Imre Z. Ruzsa,* Mathematical Institute of the Hungarian Academy of Sciences, Budapest, Pf. 127, H-1364 Hungary

MEASURE OF SUMSETS AND EJECTIVE SETS I

1   Introduction

A classical theorem of Erdős [3] in number theory asserts that if a set H of nonnegative integers is a *basis*, that is, the set

$$kH = H + \cdots + H, \quad k \text{ summands}$$

contains every nonnegative integer for some k, then the density of a sumset $A + H$ can be estimated as follows:

$$\underline{d}(A + H) \geq \underline{d}(A) + \frac{\underline{d}(A)\big(1 - \underline{d}(A)\big)}{2k}. \tag{1.1}$$

Raikov [6] proved analogous results for measures. Let G be the circle with normalized Lebesgue measure μ.

Definition 1.1 *We say that $H \subset G$ is a basis of order k for G if $kH = G$.*

Raikov shows that for an arbitrary $A \subset G$ and a basis H of order k we have

$$\underline{\mu}(A + H) \geq \underline{\mu}(A) + \frac{\underline{\mu}(A)(1 - \underline{\mu}(A))}{k}. \tag{1.2}$$

If $0 \in H$ and A is measurable (The general case of (1.2) is easily reduced to the measurable case by considering subsets of A.), then with an arbitrary $h \in H$ we have $A + H \supset A \cup (A + h)$. Hence

$$\underline{\mu}(A + H) \geq \mu\big(A \cup (A + h)\big) = \mu(A) + \mu\big((A + h)\backslash A\big). \qquad (1.3)$$

The Erdős-Raikov proof had the curious feature that in order to estimate the cardinality or measure of $A + H$, the cardinality or measure of $(A + h)\backslash A$ is shown to be large for a suitable $h \in H$. We interpret this as the amount by which the addition of h "ejects" A out of itself. This motivates the following definitions.

Definition 1.2 *By the measure of ejectivity of the set H we mean the function*

$$\zeta(x) = \zeta_H(x) = \inf_{\mu(A)=x} \sup_{h \in H} \mu\big((A + h)\backslash A\big). \qquad (1.4)$$

Then (1.3) shows that

$$\underline{\mu}(A + H) \geq \mu(A) + \zeta\big(\mu(A)\big).$$

Definition 1.3 *If $\zeta(x) = 0$ for all x, we say that H is nonejective,*
if $\zeta(x) > 0$ for some x, then H is ejective,
if $\zeta(x) > 0$ for all $x \in (0, 1)$, then H is essentially ejective.

So far we spoke about sets on the circle. Definitions 1.1-1.3 make sense in every structure with an addition and a measure. The most general situation we shall consider is when G is a unimodular locally compact group, and μ is the Haar measure. ζ is defined for those values of x that may occur as a value of μ; if G is not discrete, this means every $0 \leq x \leq \mu(G)$. We shall be interested mainly in the classical cases, the line, the circle and finite dimensional spaces, but when a more general case can be settled with little extra effort, we shall do so.

Since the function $h \mapsto \mu((A + h) \setminus A)$ is continuous, a set H is ejective (essentially ejective) if and only if the closure of H has the same property.

The principal aim of this first part is to construct nontrivial examples of ejective sets. Hence showing that our subject is nonvoid.

Raikov's theorem admits the following generalization.

Statement 1.4 *If G is compact, μ is normalized so that $\mu(G) = 1$ and H is a basis of order k for G, then we have*

$$\zeta_H(x) \geq \frac{x(1 - x)}{k}. \qquad (1.5)$$

For sake of completeness, we give a proof of this result, which is essentially the same as the Erdős-Raikov argument, in Section 2.

Thus, by 'nontrivial' we mean ejective sets that are not bases. We shall construct examples that are too small to form a basis. This will be expressed in terms of the box dimension. Let $G = \mathbb{R}/\mathbb{Z}$, that is, the unit interval with addition modulo one. (This will be more comfortable to work with than the set of unimodular complex numbers.) Let $A \subset G$, and for a positive integer n let $b(n)$ denote the minimal number of intervals of length $1/n$ that together cover A. The number

$$\beta(A) = \limsup_{n \to \infty} \frac{\log b(n)}{\log n}$$

is called the *box dimension* of A. An easy argument shows that $\beta(A) \geq 1/k$ holds for any basis of order k. (The Hausdorff dimension of a basis can be 0. Indeed, any residual set is a basis of order 2, and there are residual sets of Hausdorff dimension zero.)

Our main result is the following.

Theorem 1.5 *In $\mathbb{R}/\mathbb{Z}$ there exists an ejective set whose box dimension is 0, even*

$$b(n) < c(\log \log n)^3 \log n \tag{1.6}$$

holds for large n.

2 The Ejectivity of Bases

Lemma 2.1 *For every unimodular locally compact group G, arbitrary $H \subset G$, real x and positive integer k we have*

$$\zeta_{kH}(x) \leq k\zeta_H(x). \tag{2.1}$$

PROOF. Consider the function

$$d(u) = \mu\big((A+u)\backslash A\big).$$

We have

$$d(u+v) = \mu\big((A+u+v)\backslash A\big) \leq \mu\big((A+u+v)\backslash(A+u)\big) + \mu\big((A+u)\backslash A\big)$$
$$= d(v) + d(u).$$

(We used the translation invariance of μ, but commutativity is not assumed here.) An induction yields

$$d(h_1 + \cdots + h_k) \leq d(h_1) + \cdots + d(h_k),$$

which immediately implies (2.1).   □

Lemma 2.2 *Assume that G is compact and $\mu(G) = 1$. We have*

$$\zeta_G(x) \geq x(1 - x). \tag{2.2}$$

Proof. Take an $A \subset G$, $\mu(A) = x$. An easy application of Fubini's theorem yields

$$\int \mu\big((A + h) \cap A\big)\, d\mu(h) = x^2.$$

Consequently $\mu\big((A+h) \cap A\big) \leq x^2$ for a suitable h and then for this h we have

$$\mu\big((A + h)\backslash A\big) = \mu(A) - \mu\big((A + h) \cap A\big) \geq x(1 - x). \qquad \square$$

Proof of Statement 1.4. By the previous lemmas we have

$$\zeta_H(x) \geq \frac{1}{k}\zeta_{kH}(x) = \frac{1}{k}\zeta_G(x) \geq \frac{x(1 - x)}{k}. \qquad \square$$

3 The Measure of Ejectivity of the Whole Group

In the previous section we estimated ζ_G from below. Here we prove that this estimate is often exact.

Theorem 3.1 *Let G be an infinite compact commutative group and assume that $\mu(G) = 1$. We have*

$$\zeta_G(x) = x(1 - x). \tag{3.1}$$

We use E to denote expectation and D for the variance; that is, $D\xi = E((\xi - E\xi)^2)$.

Lemma 3.2 *Let $X_1, \ldots, X_k$ be independent real random variables, $X_i - \mathbf{E}X_i \leq K$ and*

$$\sum \mathbf{D}X_i \leq \sigma^2.$$

Write $S = \sum X_i$. For $\lambda \leq 4\sigma/K$ we have

$$\mathbf{P}(S - \mathbf{E}S \geq \lambda\sigma) \leq \exp(-\lambda^2/4). \tag{3.2}$$

Note that only a one-sided bound is required for $X_i - \mathbf{E}X_i$.
Proof. This follows from Bennett's Bernstein-type inequality [1]. His estimate for the probability in (3.2) is $\exp\big(-\lambda^2 h(\lambda K/\sigma)\big)$, where

$$h(t) = \frac{(t + 1)\log(t + 1) - t}{t^2}.$$

We obtain (3.2) by observing that $h(t) \geq 1/4$ for $t \leq 4$. $\qquad \square$

Lemma 3.3 *For every set H, its measure of ejectivity has the following properties.*

   a) $0 \le \zeta(x) \le x$ for all x.

   b) $|\zeta(x) - \zeta(y)| \le |x - y|$ for all x, y.

   c) If G is compact and $\mu(G) = 1$, then $\zeta(x) = \zeta(1 - x)$ for all x.

PROOF. Property a) is obvious. To prove part b), assume that $x < y$. For a set A such that $\mu(A) = x$ and $\mu\big((A + h)\backslash A\big) < \zeta(x) + \varepsilon$ for every $h \in H$, take any $B \supset A$, $\mu(B) = y$. We have

$$(B + h)\backslash B \subset \big((A + h)\backslash A\big) \cup \big((B\backslash A) + h\big)$$

which shows $\mu\big((B+h)\backslash B\big) \le \zeta(x) + \varepsilon + (y - x)$ and hence $\zeta(y) \le \zeta(x) + y - x$. The inequality $\zeta(x) \le \zeta(y) + y - x$ can be proved similarly, by applying the inclusion

$$(A + h)\backslash A \subset \big((B + h)\backslash B\big) \cup (B\backslash A).$$

To prove part c), take a set A such that $\mu(A) = x$ and consider the set $B = G\backslash A$. It satisfies $\mu(B) = 1 - x$ and $(B + h)\backslash B = A\backslash(A + h)$. Hence $\mu\big((B + h)\backslash B\big) = \mu\big((A + h)\backslash A\big)$. $\qquad\square$

Lemma 3.4 *Let G be a finite group, $|G| = m$, $\mu(G) = 1$. For every $x = k/m$, where $0 \le k \le m$ is an integer, we have*

$$\zeta_G(x) \le x(1 - x)\left(1 + c\sqrt{\frac{\log m}{m}}\right) \tag{3.3}$$

with an absolute constant c.

PROOF. By property c) above, it suffices to consider $x \le 1/2$. Write $x(1-x) = y$.

Let ξ_g, $g \in G$ be independent 0-1 valued random variables that assume 1 with probability x. Let

$$B = \{g \in G : \xi_g = 1\},$$

a random set. We have

$$|B| = \sum \xi_g,$$

which has a binomial distribution. Hence

$$\mathbf{P}(|B| = k) = \binom{m}{k} x^k (1 - x)^{n-k} \ge 1/(m + 1).$$

(The last inequality follows from the fact that this is the maximal term in the binomial distribution and the sum of all $m+1$ terms is 1.)

Now we consider $B \cap (B+h)$ for $h \in G, h \neq 0$. We have

$$\eta = |B \cap (B+h)| = \sum_{g \in G} \xi_g \xi_{g-h}.$$

This is a sum of m random variables, each of which assumes 1 with probability x^2 and 0 otherwise. Hence $\mathbf{E}\eta = mx^2$. The terms are not all independent. First we show that we can decompose G as $G = G_1 \cup G_2 \cup G_3$ so that in the corresponding decomposition of η,

$$\eta = \eta_1 + \eta_2 + \eta_3, \quad \eta_i = \sum_{g \in G_i} \xi_g \xi_{g-h},$$

each η_i is a sum of independent variables. (This decomposition will depend on h.) This will happen if for all $g, g' \in G_i, g \neq g'$, the elements $g, g-h, g', g'-h$ are all different, which is equivalent to saying that $h \notin G_i - G_i$. Now let H be the subgroup generated by h, $l = |H|$ the order of h, and consider the decomposition of G into left cosets of H:

$$G = \bigcup_{k=1}^{m/l} (r_k + H).$$

We define for $i = 1, 2$

$$G_i = \{r_k + jh : 1 \leq k \leq m/l, 1 \leq j \leq l-1, j \equiv i \pmod 2\}$$

and

$$G_3 = \{r_k : 1 \leq k \leq m/l\}.$$

Now we apply Lemma 3.2 for the variables $X_g = -\xi_g \xi_{g-h}$. Recall that X_g assumes the values 0 and -1, 0 with probability $1-x^2$ and -1 with probability x^2. Hence $\mathbf{E}X_g = -x^2$ and $\mathbf{D}X_g = x^2(1-x^2) \leq x^2$, and the assumptions are fulfilled with $K = x^2$ and $\sigma^2 = mx^2$. Thus up to $\lambda \leq 4\sqrt{m}/x$ we have

$$\mathbf{P}(\eta_i - \mathbf{E}\eta_i \leq -\lambda x \sqrt{m}) \leq \exp(-\lambda^2/4).$$

We put $\lambda = 4\sqrt{\log m}$; this is in the permissible range since $\log m < m$. We obtain that

$$\mathbf{P}(\eta_i - \mathbf{E}\eta_i \leq -4\sqrt{\log m} x \sqrt{m}) \leq m^{-4}.$$

Consequently

$$\mathbf{P}(\eta - \mathbf{E}\eta \leq -12\sqrt{\log m} x \sqrt{m}) \leq 3m^{-4}.$$

MEASURE OF SUMSETS AND EJECTIVE SETS I159

Recall that $\eta - \mathbf{E}\eta = |B \cap (B+h)| - x^2 m$. Since there are $< m$ possible choices of h, the probability that

$$|B \cap (B+h)| \leq x^2 m - 12x\sqrt{m\log m}$$

for some h is less that $3m^{-3} < 1/(m+1)$ if $m \geq 3$. Consequently there is a choice of B that satisfies both $|B| = k$ and

$$|B \cap (B+h)| \geq x^2 m - 12x\sqrt{m\log m}$$

for all h. Whence

$$|(B+h)\backslash B| = |B| - |B \cap (B+h)| \leq mx(1-x)\left(1 + 24\sqrt{\frac{\log m}{m}}\right).$$

(We used the fact that $x \leq 1/2$.) $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

Lemma 3.5 *Let G be the circle (additive group of reals modulo 1). We have $\zeta_G(x) = x(1-x)$ for every $0 \leq x \leq 1$.*

PROOF. Take two positive integers $k \leq m$. Let G' be the additive group of residue classes modulo m, which we identify with the integers $0, 1, \ldots, m-1$. Take a set $B' \subset G'$ with the properties $|B'| = k$ and

$$|(B'+h)\backslash B'| \leq k(1-k/m)\left(1 + c\sqrt{\frac{\log m}{m}}\right) \qquad\qquad (3.4)$$

for every h; the existence of such a set follows from the previous lemma.

Now define a set $B \subset G$ by

$$B = \bigcup_{j\in B'}\left[\frac{j}{m}, \frac{j+1}{m}\right).$$

For a number of the form $h = r/m$, $0 \leq r \leq m-1$ integer, we have

$$\mu\big((B+h)\backslash B\big) = \frac{1}{m}|(B'+r)\backslash B'|$$

and this measure is a linear function of h between r/m and $(r+1)/m$. Hence (3.4) implies

$$\mu\big((B+h)\backslash B\big) \leq \frac{k}{m}\left(1 - \frac{k}{m}\right) + c\sqrt{\frac{\log m}{m}}$$

for all h. We conclude that

$$\zeta_G(k/m) \leq \frac{k}{m}\left(1 - \frac{k}{m}\right) + c\sqrt{\frac{\log m}{m}}$$

for every $k \leq m$. By property b) of Lemma 3.3 we conclude that $\zeta_G(x) \leq x(1-x)$ for every $x \in [0,1]$. □

Proof of Theorem 3.1. Let G be an arbitrary compact group and G' a factor-group of G, with the natural homomorphism $\phi : G \to G'$. Take any $B' \subset G'$ and let $B = \phi^{-1}(B')$. For every $h \in G$ we have

$$\mu\big((B+h)\backslash B\big) = \mu'\big((B' + \phi(h))\backslash B'\big).$$

Hence we have $\zeta_G(x) \leq \zeta_{G'}(x)$ for every x assumed by μ'.

Now let G be an infinite commutative compact group. If G has a factor isomorphic to the circle, then we obtain $\zeta_G(x) \leq x(1-x)$ by the above observation and Lemma 3.5. If this is not the case, then G has arbitrarily large finite factors. Then the above observation and Lemma 3.4 yield

$$\zeta_G(k/m) \leq \frac{k}{m}\left(1 - \frac{k}{m}\right) + c\sqrt{\frac{\log m}{m}}$$

for any m that can appear as a size of a finite factor, and for all $k \leq m$. By property b) of Lemma 3.3 we conclude that $\zeta_G(x) \leq x(1-x)$ for every $x \in [0,1]$. Together with Lemma 2.2 we get the desired conclusion. □

4   A Criterion for Ejectivity

In this section let G be a commutative group. Unlike in the previous sections, we do not assume G to be compact. Thus the Haar measure may be infinite.

For a measure ν on G, we use $\hat{\nu}$ to denote its Fourier transform, that is,

$$\hat{\nu}(\gamma) = \int \gamma \, d\nu$$

for any character γ of G.

We use G^* to denote the group of characters, and $d\gamma$ for integration on G^* with respect to its Haar measure μ^*. We assume that μ and μ^* are normed so that in Plancherel's formula the constant is 1.

Theorem 4.1 *Assume that $H \subset G$ and there exists a probability measure ν supported on the closure of H such that*

$$\mu^*(\{\gamma : \operatorname{Re}\hat{\nu}(\gamma) > 1 - \eta\}) = v < \infty$$

with some constant $\eta > 0$. Then for every $x \leq 1/v$ we have

$$\zeta_H(x) \geq \eta x(1 - vx). \tag{4.1}$$

In particular, H is ejective. If for every $\varepsilon > 0$ we can achieve $v < \varepsilon$ with a suitable ν and η (which may depend on ε), then H is essentially ejective.

PROOF. Replacing H by its closure does not affect (essential) ejectivity. Therefore we may assume that H itself is closed.

Take a set $A \subset G$, $\mu(A) = x$ and let f denote the indicator function of A. We have

$$f(t - h) - f(x) = \begin{cases} 1 & \text{if } t \in (A + h)\backslash A, \\ -1 & \text{if } t \in A\backslash(A + h), \\ 0 & \text{otherwise.} \end{cases}$$

Consequently

$$\int |f(t - h) - f(t)|^2 d\mu(t) = 2\mu\big((A + h)\backslash A\big). \tag{4.2}$$

The Fourier transform of f is

$$F(\gamma) = \int f(t)\gamma(t)d\mu(t) = \int_A \gamma \, d\mu,$$

and that of the function $f(t - h)$ is

$$\int f(t - h)\gamma(t)d\mu(t) = F(\gamma)\gamma(h).$$

Hence an application of Plancherel's identity to (4.2) yields

$$2\mu\big((A + h)\backslash A\big) = \int |F(\gamma)\big(\gamma(h) - 1\big)|^2 \, d\gamma.$$

Since $|z - 1|^2 = 2(1 - \operatorname{Re} z)$ whenever $|z| = 1$, we obtain

$$\mu\big((A + h)\backslash A\big) = \int |F(\gamma))|^2\big(1 - \operatorname{Re}\gamma(h)\big) \, d\gamma. \tag{4.3}$$

Now we integrate (4.3) with respect to ν; this yields

$$\int \mu\big((A + h)\backslash A\big) \, d\nu(h) = \int |F(\gamma)|^2 \int \big(1 - \operatorname{Re}\gamma(h)\big) \, d\nu(h) \, d\gamma$$

$$= \int |F(\gamma)|^2 \big(1 - \operatorname{Re}\hat{\nu}(\gamma)\big) \, d\gamma \tag{4.4}$$

$$\geq \eta \int_{\operatorname{Re}\hat{\nu}(\gamma) \leq 1 - \eta} |F(\gamma)|^2 \, d\gamma.$$

Again by Plancherel's formula we know that $\int |F(\gamma)|^2 \, d\gamma = \mu(A) = x$ and $|F(\gamma)| \le x$ for each γ. Hence

$$\int_{\operatorname{Re} \hat{\nu}(\gamma) \le 1-\eta} |F(\gamma)|^2 \, d\gamma \ge x - vx^2.$$

By substituting this into (4.3) we obtain

$$\int \mu\big((A+h)\backslash A\big) \, d\nu(h) \ge \eta x(1 - vx).$$

Since the supremum of $\mu\big((A+h)\backslash A\big)$ is not less than its ν-mean, the theorem is proved. $\qquad\square$

We formulate separately the case of compact groups.

Theorem 4.2 *Let G be a compact commutative group and $\mu(G) = 1$. Assume that $H \subset G$ and there exists a probability measure ν supported on the closure of H such that $\operatorname{Re} \hat{\nu}(\gamma) \le 1-\eta$ for every character γ with at most k exceptions for some constant $\eta > 0$. Then for every x we have*

$$\zeta_H(x) \ge \eta x(1 - kx). \tag{4.5}$$

In particular, H is ejective. If $k = 1$, that is, the only exception is the principal character, then

$$\zeta_H(x) \ge \eta x(1 - x) \tag{4.6}$$

and H is essentially ejective.

Remark 4.3 *By the previous theorem, if H is a nonejective set in the circle group, then every probability measure ν supported on the closure of H satisfies*

$$\limsup_{n \to \infty} \operatorname{Re} \hat{\nu}(n) = 1.$$

This condition is easily seen to be equivalent to the condition

$$\limsup_{n \to \infty} |\hat{\nu}(n)| = 1.$$

That is, a nonejective Borel set is a weak Dirichlet set (see [2], [4], [5]).

One can show that, for closed sets, the weak Dirichlet property is actually equivalent to nonejectivity. (The proof of this fact will be presented elsewhere.) On the other hand, a closed set is weak Dirichlet if and only if it is an N-set (see [4, Theorem 2.5] or [2, Corollary 8.11]). Therefore,

H is nonejective $\iff$ cl H is weak Dirichlet $\iff$ cl H is an $N-$set,

where cl H denotes the closure of H.

5 Proof of Theorem 1.5

We construct a set B satisfying (1.6).

We shall obtain B as the intersection of a decreasing sequence B_k of sets. We build B_k in the following way. We define a sequence m_k of integers such that $m_k | m_{k+1}$ for all k, another sequence b_k such that $1 \leq b_k \leq m_k$, a set $J_k \subset [0, m_k - 1]$ of integers with $|J_k| = b_k$ and put

$$B_k = \bigcup_{j \in J_k} \left[\frac{j}{m_k}, \frac{j+1}{m_k} \right).$$

The numbers m_k, b_k will be given in the course of the proof.

To establish the ejectivity of B we are going to apply Theorem 4.2. The characters of the circle group $G = \mathbb{R}/\mathbb{Z}$ are the functions

$$\gamma_r(x) = e(rx) = e^{2\pi i r x}.$$

Correspondingly, the Fourier transform of a measure ν is the function

$$\hat{\nu}(r) = \int e(rx) \, d\nu(x).$$

We shall construct measures ν_k on B_k satisfying

$$|\hat{\nu}_k(r)| \leq \eta_k = \frac{1}{2} - \frac{c}{\sqrt{k}} \tag{5.1}$$

for $k > k_0$ and $r \neq 0$.

Our measure ν_k will be the normalized restriction of the Lebesgue measure to the sets B_k. The Fourier transform of this measure is

$$\hat{\nu}_k(r) = \frac{m_k}{b_k} \sum_{j \in J_k} \int_{j/m_k}^{(j+1)/m_k} e(rx) \, dx.$$

This is connected to the sum

$$g_k(r) = \frac{1}{b_k} \sum_{j \in J_k} e(jr/m_k)$$

via the formula

$$\hat{\nu}_k(r) = e\left(\frac{r}{2m_k} \right) \frac{\sin \pi r/m_k}{\pi r/m_k} g_k(r).$$

In particular, $|\hat{\nu}_k(r)| \le |g_k(r)|$ for all r, and $|\hat{\nu}_k(r)| = 0$ if $m_k|r$ and $r \ne 0$. Observe that $g_k(r)$ is periodic with period m_k. Hence to ensure (5.1) it is sufficient to achieve

$$|g_k(r)| \le \eta_k \text{ for } 1 \le r \le m_k - 1. \tag{5.2}$$

Write $n_k = m_{k+1}/m_k$. The condition $B_{k+1} \subset B_k$ holds if each element of J_{k+1} is of the form

$$j = n_k j' + q, \quad j' \in J_k, \ 0 \le q \le n_k - 1. \tag{5.3}$$

We construct the sets J_k recursively. Suppose that J_k is given, and it satisfies (5.2). We find J_{k+1} so that (5.2) holds also for $k+1$, assuming that certain growth conditions hold for m_k and b_k.

Let

$$\varrho = \frac{b_{k+1}}{b_k n_k}.$$

We select each number j of the form (5.3) into J_{k+1} independently, with probability ϱ. Then

$$\mathbf{E}|J_{k+1}| = \varrho n_k |J_k| = b_{k+1}$$

and

$$\mathbf{P}\big(|J_{k+1}| = b_{k+1}\big) = \binom{b_k n_k}{b_{k+1}} \varrho^{b_{k+1}} (1 - \varrho)^{b_k n_k - b_{k+1}}$$

$$\ge (1 + b_k n_k)^{-1} \ge (1 + m_{k+1})^{-1}$$

by the same argument as we used in Section 3.

For any j of the form (5.3), let ξ_j be the indicator of J_{k+1}; these are independent random variables, each assuming 1 with probability ϱ and 0 with probability $1 - \varrho$. We can express the Fourier series of J_{k+1} as follows.

$$g_{k+1}(r) = \frac{1}{b_{k+1}} \sum_{j \in J_{k+1}} e\left(\frac{rj}{m_{k+1}}\right) = \frac{1}{b_{k+1}} \sum \xi_j e\left(\frac{rj}{m_{k+1}}\right).$$

For a number expressed in the form (5.3) we have

$$\frac{j}{m_{k+1}} = \frac{j'}{m_k} + \frac{q}{m_{k+1}}.$$

Hence the expectation of $g_{k+1}(r)$ is

$$\mathbf{E}g_{k+1}(r) = \frac{\varrho}{b_{k+1}} \sum_{j' \in J_k} \sum_{q=0}^{n_k - 1} e\left(\frac{rj'}{m_k} + \frac{rq}{m_{k+1}}\right) = \frac{1}{n_k} \sum_{q=0}^{n_k - 1} e\left(\frac{rq}{m_{k+1}}\right) g_k(r).$$

Consequently $|\mathbf{E}g_{k+1}(r)| \leq |g_k(r)|$ for all r, and it is $= 0$ if $m_k|r$ but $m_{k+1} \nmid r$. We can conclude by the inductive assumption that

$$|\mathbf{E}g_{k+1}(r)| \leq \eta_k \text{ for } 1 \leq r \leq m_{k+1} - 1. \qquad (5.4)$$

To estimate the deviation from the mean we apply Lemma 3.2 separately for the four variables $\pm\xi_j \cos(rj/m_{k+1})$ and $\pm\xi_j \sin(rj/m_{k+1})$. The parameters will be chosen as $K = 1$, $\sigma^2 = \varrho n_k b_k = b_{k+1}$ and $\lambda = 4\sqrt{\log m_{k+1}}$ so that $\exp(-\lambda^2/4) = m_{k+1}^{-4}$. The condition $\lambda \leq 4\sigma/K$ becomes

$$\log m_{k+1} \leq b_{k+1}. \qquad (5.5)$$

Since $|z| \leq |\operatorname{Re} z| + |\operatorname{Im} z|$, these four inequalities imply

$$\mathbf{P}\big(|g_{k+1}(r) - \mathbf{E}g_{k+1}(r)| \geq \delta\big) \leq m_{k+1}^{-4},$$

where

$$\delta = 2\frac{\lambda\sigma}{b_{k+1}} = 8\sqrt{\frac{\log m_{k+1}}{b_{k+1}}}.$$

Since there are $m_{k+1} - 1$ possible choices of r, the probability that

$$|g_{k+1}(r) - \mathbf{E}g_{k+1}(r)| \geq \delta$$

happens for at least one r is less than m_{k+1}^{-3}. This is less than the probability that $|J_{k+1}| = b_{k+1}$. Thus there is a choice that satisfies both $|J_{k+1}| = b_{k+1}$ and

$$|g_{k+1}(r) - \mathbf{E}g_{k+1}(r)| < \delta$$

for all $1 \leq r \leq m_{k+1} - 1$. Hence, using (5.4) we obtain

$$|g_{k+1}(r)| \leq \eta_k + \delta,$$

and the induction works if

$$\eta_k + \delta \leq \eta_{k+1}. \qquad (5.6)$$

Now we put $m_k = 2^{2^k}$ for all k and $b_k = k^3 2^k$ for $k > k_0$, $b_k = m_k$ for $1 \leq k \leq k_0$. Hence b_k/m_k will be decreasing and condition (5.5) is satisfied. We get

$$\delta = 8\sqrt{\log 2}(k+1)^{-3/2},$$

while

$$\eta_{k+1} - \eta_k = \frac{c}{\sqrt{k}} - \frac{c}{\sqrt{k+1}} \geq \frac{c}{2}(k+1)^{-3/2}.$$

Thus (5.6) holds if we take, say, $c = 16$.

We start the induction from $k = k_0$. Here $J_k = \{0, 1, \ldots, m_k - 1\}$. Thus $g_k(r) = 0$ for all $1 \leq r \leq m_k - 1$. Therefore we only need that $\eta_{k_0} \geq 0$, that is, $c/\sqrt{k_0} \leq 1/2$.

Having defined the sequences B_k and ν_k, we put $B = \cap B_k$. We can estimate $b(n)$, the number of intervals of length $1/n$ that cover B, as follows. If $m_{k-1} < n \leq m_k$, then the b_k intervals that constitute B_k cover B. Thus

$$b(n) \leq b_k = k^3 2^k \ll (\log \log n)^3 \log n.$$

To establish that B is ejective, take any convergent subsequence (in the weak topology) ν_{k_j} of the sequence ν_k. The limit ν of this sequence is a probability measure supported on B such that $|\hat{\nu}(r)| = \lim |\hat{\nu}_{k_j}(r)| \leq \lim \eta_k = 1/2$ for every $r \neq 0$. Hence B is essentially ejective by Theorem 4.2. $\qquad\square$

Remark 5.1 *In the proof above we have constructed a compact set B of box dimension zero such that B supports a probability measure ν with $\sup_n \operatorname{Re} \hat{\nu}(n) < 1$. This implies that B is not an N-set. On the other hand, the group generated by B is the countable union of closed sets of box dimension zero. In this way we constructed a compact set B with the following properties:*

(i) *B generates a proper F_σ subgroup of the circle group; and*

(ii) *B is not an N-set.*

References

[1] G. Bennett, *Probability inequalities for the sum of independent random variables*, J. American Statist. Assoc., **57** (1962), 33–45.

[2] L. Bukovský, N. N. Kholshchevnikova and M. Repický, *Thin sets of harmonis analysis and infinite combinatorics*, Real Analysis Exchange, **20**(2) (1994-5), 454–509.

[3] P. Erdős, *On the arithmetical density of the sum of two sequences, one of which forms a basis for the integers*, Acta Arithmetica, **1** (1936), 201–207.

[4] B. Host, J. F. Méla and F. Parreau, *Non singular transformations and spectral analysis of measures*, Bull. Soc. Math. France, **119** (1991), 33–90.

[5] S. Kahane, *Antistable classes of this sets in harmonis analysis*, Illinois J. of Math., **37** (1993), 186–223.

[6] D. A. Raikov, *On the addition of point sets in the sense of Schnirelmann*, Mat. Sbornik, 5(47) (1939), 425–440, (in Russian).