JOHN A. HAIGHT

An $F_\sigma$ semigroup of zero measure which contains a translate of every countable set


<http://www.numdam.org/item?id=TAN_1984-1985__1__A11_0>
AN $F_\sigma$ SEMIGROUP OF ZERO MEASURE WHICH CONTAINS A TRANSLATE OF EVERY COUNTABLE SET

by John A. HAIGHT (*)

In 1942, PICCARD [10] gave an example of a set of real numbers whose sum set has zero Lebesgue measure but whose difference set contains an interval. About thirty years later, various authors (CONNOLLY, JACKSON, WILLIAMSON and WOODALL) in a series of papers constructed $F_\sigma$ sets $E \subseteq \mathbb{R}$ such that $E - E$ contains an interval while $m((k)E) = 0$ for progressively larger values of $k$, where

$$(k)E = \{x_1 + x_2 + \cdots + x_k ; \, x_i \in E \, , \, 1 \leq i \leq k\} .$$

These authors' interest was in an approach to the construction of asymmetric Raikov systems, [5], defined as follows.

If $G$ is a locally compact abelian group, a Raikov system is a family $\mathcal{S}$ of $F_\sigma$ subsets satisfying the following conditions :

(a) If $F_1 , F_2 , \ldots \in \mathcal{S}$ then $\bigcup_{n=1}^{\infty} F_n \in \mathcal{S} .$

(b) If $F_1 \subseteq F_2 \in \mathcal{S}$ and $F_1$ is $F_\sigma$ then $F_1 \in \mathcal{S} .$

(c) If $F_1 , F_2 \in \mathcal{S}$ then $F_1 + F_2 \in \mathcal{S} .$

A Raikov system is said to be asymmetric if $\Lambda \in \mathcal{S}$ does not necessarily imply $-\Lambda \in \mathcal{S} .$

CONNOLLY and WILLIAMSON [3] noted that the existence in $\mathbb{R}$ of an asymmetric Raikov system was equivalent to the existence of an $F_\sigma$ semigroup of zero Lebesgue measure which is not contained in any proper subgroup of $\mathbb{R}$, which in turn is equivalent to the existence of an $F_\sigma$ set $E$ such that $E - E = \mathbb{R}$, but $m((k)E) = 0$ for $k = 1 , 2 , \ldots$ I was able to solve this problem, although unfortunately the central idea was rather obscured by technical details. Recently, however, BROWN and MORAN [1] have simplified my proof. The results of this paper are a generalization of this simplification.

If $\mathcal{R}$ is a ring and $\alpha , \beta \in \mathcal{R}$ and $E , F \subseteq \mathcal{R}$, we write

$$\alpha \cdot E + \beta \cdot F = \{\alpha \cdot x + \beta \cdot y ; \, x \in E , \, y \in F\} ;$$

if $E$ is finite, $|E|$ denotes the number of elements in $E$. In this notation, the statement $E - E = \mathbb{R}$ is equivalent to the statement that, for every $F \subseteq \mathcal{R}$ such

(*) John A. HAIGHT, Department of Mathematics, University College, Gower Street, LONDON WC 1 E 6BT (Grande-Bretagne).
that $|F| \leq 2$, there is a $c \in \mathbb{R}$ such that $F + \{c\} \subseteq B$. (From now on, we shall write "c" instead of "\{c\}". This leads to the question: If $(k) E$ is 'small', how "large" is the family of sets $F$ that can be translated into $E$?

For any $n \in \mathbb{N}$, we write $I(n) = \{0, \ldots, n-1\}$ and $\mathbb{Z}(n)$ for the integers modulo $n$.

**Theorem 1.** For all $j$, $n \in \mathbb{N}$ and $\varepsilon > 0$, there is an $N = N(j, n, \varepsilon)$ such that for any $N \geq N$, there is a subset $A$ of $\mathbb{Z}(N)$ such that

(a) If $F \subseteq \mathbb{Z}(j)$, $|F| \leq n$, there is a $c = c(F)$ such that $F + c \subseteq A$.
(b) $|A| N^{-1} < \varepsilon$.

If $F \subseteq I(n)^N$, $i = 1, 2, \ldots$, for some $n > 1$, we shall say that the set $C = \{z_i = x_i \mod n \mid x_i \in F\}$ is a Cantor set. If $|F|^N \leq r$, we shall say $C \in b(\mathbb{Z}(n), r)$. If $F_i = F$, $i = 1, 2, \ldots$, we shall say that $C(e \in b(n, |F|))$ is self-similar.

**Theorem 2.** For any $n$, $r$, $j \in \mathbb{N}$ and $\varepsilon > 0$, there is an $N = N(j, n, \varepsilon)$ and a self-similar Cantor set $K \subseteq \mathbb{R}^N$ such that

(a) For any $F \in b(n, r)$, there is a $d = d(F)$ such that $F + d \subseteq K$.
(b) $(j)K \in b(n, \varepsilon N)$.

We note that (a) implies that if $F$ is any finite set containing not more than $r$ points, then there is a $c$ such that $F + c \subseteq K$.

**Theorem 3.** There is an $F_\omega$ set $E \subseteq \mathbb{R}^N$ such that

(a) If $F \subseteq \mathbb{R}^N$ is a countable set, there is a $c = c(F)$ such that $F + c \subseteq E$.
(b) For any $k \in \mathbb{N}$, $m((k) E) = 0$.

Cassels [2] proved that if $\lambda_1, \ldots, \lambda_r$ are real numbers, there is a number $\varphi$ such that $\|\varphi + \lambda_i u\| > c/u$, $u \in \mathbb{N}$, $i = 1, \ldots, r$ ($\|x\|$ denotes the distance of $x$ from the nearest integer to $x$, $c = c(r)$).

In our notation $\{\lambda_1, \ldots, \lambda_r\} + \alpha \in B_r$ $B_r = \{x; \|x\| > c(r)\}; u, u \in \mathbb{N}\}$.

Let $B = \bigcup_{n=1}^{\infty} B_n$; then $B$ is the set of "badly approximable numbers". It is well-known that $B = \bigcup_{n=1}^{\infty} F(n)$ where $F(n)$ is the set of numbers whose continued fraction expansions have partial quotients $\leq n$ and that $m(B) = 0$. However, (2) $B = \mathbb{C}$. Indeed K. Hall [7] proved that (2) $F(4) = \mathbb{C}$ (more recently SLA showed (4) $F(2) = \mathbb{C}$). Davenport and Schmidt [4], [11] extended Cassels' result in various ways. In particular, Schmidt's theorem implies that, for every countable $\mathbb{R}^N$ there is an $\omega \in \mathbb{R}^N$ (actually many such $\omega$) such that $F + \omega \subseteq B$ where $B$ in $\mathbb{R}^N$ is defined as

$$\{x = (x_1, \ldots, x_n); \max(\|ux_1\|, \ldots, \|ux_n\|) < c(x) u^{-1/n}\}.$$
Again $m(B) = 0$, and $(2) B = \mathbb{R}^n$.

Proof of Theorems.

**Lemma 1.** - For all $j, n \in \mathbb{N}$ and $\epsilon > 0$, there is an $N = N(j, n, \epsilon)$ and a subset $A$ of $\mathbb{Z}(n)$ such that

(a) If $F \subseteq \mathbb{Z}(n)$, $|F| \leq n$, there is a $c = c(F)$ such that $F + c \subseteq A$.

(b) $|(j)A| N^{-1} < \epsilon$.

If $x, y \in \mathbb{R}^n$ for some $n \geq 1$, write

$$x.y = x_1 y_1 + \cdots + x_n y_n.$$

**Lemma 2.** - Given $k, j, n \in \mathbb{N}$ and $\epsilon > 0$, there is an $N = N(k, j, n, \epsilon)$ such that for each $j \in I(n)^n$, there is $c = c(j) \in I(n)$, such that if $c = (c, \ldots, c)$ and

$$E = E(n, N) = \{x; x \in I(n), x \equiv g(j + c^*) \mod N, g \in I(n)^n, j \in I(n)^n\},$$

then $|(j)E| N^{-1} < \epsilon$.

If $h > 2$ this is stronger than lemma 1. For if $F = \{i_1, \ldots, i_n\}$, then $j = (j_1, \ldots, j_n) \in I(n)^n$ and, taking $g(i) = (0, \ldots, i^{(i)}\text{th place}), \ldots, 0)$, we have $g(i) \in I(n)^n$, and so $g(i)(j + c^*) \in E$, that is $j_1 + c \in E$, $i = 1, \ldots, n$.

Proof of Lemma 2. - Fix $n$. We use induction on $j$. Assume the lemma holds for some $j$ and for all $k, n$. Given $k, n, \epsilon$, let $T = N(2k, j, n, \epsilon/2)$. Let

$$G = \{g; g: F \rightarrow I(n)^n \setminus \{(0, \ldots, 0)\}, F \subseteq I(T)^n, 0 < |F| \leq j + 1\}.$$

Let $\lambda = |G|$, and let $\varphi: I(\lambda) \rightarrow G$ be a bijection.

Now choose primes $P_0 < P_1 < \cdots < P_{\lambda-1}$ such that

(a) $P_0 > nMT$,

(b) $\sum_{1 \leq i \leq \lambda-1} \frac{1}{P_i} < \epsilon/2$.

Let $P = P_0 \times \cdots \times P_{\lambda-1}$ and let $S = P^\times$.

For $j \in I(S)^n$, let $j' \in I(T)^n$, where $j'_1 = j_1 \mod T$, we choose $c(f)$ to satisfy (1) and (2)

(1) $c(j) = c(j') \mod T$

(2) $\varphi(r)(j')(j + c^*(j)) = 0 \mod P_r$

if $j' \in \text{dom} \varphi(r)$, otherwise let $c(j) = 0 \mod P_r$, $r = 0, \ldots, \lambda - 1$.

We need to show that (2) is possible. If $j' \in \text{dom} \varphi(r)$, then $\varphi(r)(j') = \lambda$ say, where $\lambda \in I(n)^n \setminus \{(0, \ldots, 0)\}$ so
$$\varphi(r)(j^*)(j + c^*(j^*)) = \lambda(j + c^*) = \lambda_1 j_1 + \cdots + \lambda_n j_n + c(j)(\lambda_1 + \cdots + \lambda_n)$$

Now 0 < \(\lambda_1 + \cdots + \lambda_n \leq n\) so condition (b) ensures that we can find \(c(j)\) so that the above equation is congruent to zero mod \(P_r\).

Now if \(x \in (j+1)E(\mathbb{H}, S)\),

\[x = \sum_{i=1}^{j+1} \lambda(i)(j(i) + c^*(j(i))) \text{ mod } S\]

for some \(\lambda(i) \in I(\mathbb{H})^n\) and \(j(i) \in I(j)^n\), \(i = 1, \ldots, j+1\).

We have two cases:

**Case 1.** \(- j(s)^* = j(t)^*\) for some \(s \neq t\). Then

\[x = \sum_{i=1}^{j+1} \lambda(i)(j(i) + c^*(j(i)))\]

\[= \sum_{1 \leq i \leq j+1, i \neq s, t} \lambda(i)(j(i) + c^*(j(i))) + \lambda(s)(j(s) + c^*(j(s))) + \lambda(t)(j(t) + c^*(j(t)))\]

so \(x \in (j)E(2^M, T) + T\mathbb{Z}\).

**Case 2.** \(- j(s)^* = j(t)^*\) only if \(s = t\). Then there is an \(r, 0 < r \leq j - 1\), such that

\[\varphi(r)(j(i)^*) = \lambda(i)\text{ for } i = 1, \ldots, j+1\]

So

\[x = \sum_{i=1}^{j+1} \varphi(r)(j(i)^*)(j(i) + c^*(j(i))) \in P_r\mathbb{Z}\]

Thus we have

\[(j+1)E(\mathbb{H}, S) + S\mathbb{Z} \subseteq \left( \bigcup_{r=0}^{j-1} P_r\mathbb{Z} \right) u \left( (j)E(2^M, T) + T\mathbb{Z} \right) + S\mathbb{Z},\]

so \(|(j+1)E(\mathbb{H}, S)| < \varepsilon/2 + \varepsilon/2 = \varepsilon\).

We modify the argument for \(j = 0\): take \(T = 1\) and \(G = I(\mathbb{H})^n \setminus \{(0, \ldots, 0)\}\) and use (2) (only) to define \(c(j)\). Then if \(x \in E(\mathbb{H}, S)\),

\[x = \lambda(j + c^*(j)) = \varphi(r)(j + c^*(j))\text{ for some } r\]

So \(x \in \bigcup_{0 \leq r \leq j-1} P_r\mathbb{Z}\).

**Lemma 3.** For any \(j, n \in \mathbb{N}\) and \(\varepsilon > 0\), there is an \(N \in \mathbb{N}\) and an \(E \subseteq T\) (where \(T\) is \(R\) modulo 1) such that

(1) \(E\) consists of a finite union of closed intervals.

(2) If \(G \subseteq T\) and \(|G| < n\), there is a \(d = d(G)\) such that \(G + d \subseteq E\).

(3) \(\mu((j)E + r^{-1}(0, 5j)) < \varepsilon\) for all \(r > N\).

The difference between Lemma 1 and Theorem 1 is that the modulus of Lemma 1 has to be the product of very large primes. We need Lemma 3 to show that, rather surprisingly, any sufficiently large modulus will do.
Proof of Lemma 3 (assuming Lemma 1). - Let $T = N(j, n, c/6j)$, where $N$ is as in Lemma 1. Let $E = N^{-1} A + (0, N^{-1})$. We show that $E$ has the required properties

$$(j)E + r^{-1}(0, 5j))$$

$$= (j) N^{-1} A + (0, jN^{-1}) + (0, 5j r^{-1}) \subseteq (j) N^{-1} A + (0, 6j N^{-1})$$

so $n((j) E + r^{-1}(0, 5j)) \leq |(j) A| \times 6j/N < c$.

Now $G$ can be covered by at most $n$ intervals of the form $(i/N, (i+1)/N)$, $i \in \mathbb{Z}$ so

$$G \subseteq N^{-1} F + (0, N^{-1}) \text{ for some } F \subseteq 2(N) \text{ where } |F| \leq n.$$ 

If $c = c(F)$, we have

$$G + c/N \subseteq N^{-1}(F + c) + (0, N^{-1}) \subseteq N^{-1} A + (0, N^{-1}) = E,$$

which gives (2), taking $d = c/N$.

Proof of Theorem 1 (assuming Lemma 3). - Since $E$ is a finite union of closed intervals,

$$E = \bigcup_{i=1}^{k} (x_i + (0, \delta_i)) \text{ for some } x_1, \ldots, x_k \text{ and } \delta_1, \ldots, \delta_k.$$ 

If $M \geq N$, then

$$E + (0, M^{-1}) = \bigcup_{i=1}^{k} ((x_i, (x_i + 1/M)) + (0, \delta_i))$$

$$= \bigcup_{i=1}^{k} (y_i M^{-1} + (0, \delta_i)) \text{ for } y_i = (M x_i + 1), \ i = 1, \ldots, k$$

$$= \bigcup_{i=1}^{k} (z_i M^{-1} + (0, z_i M^{-1})) \text{ where } z_i = [N \delta_i], \ i = 1, \ldots, k$$

$$= \bigcup_{i=1}^{k} (y_i M^{-1} + M^{-1}(z_i) + (0, M^{-1}))$$

$$= M^{-1} B + (0, M^{-1}) \ldots \ (A)$$

where $B = \bigcup_{i=1}^{k} (y_i + I(z_i))$.

Now

$$M^{-1} B + (0, 3/M) = \bigcup_{i=1}^{k} (y_i M^{-1} + M^{-1}(0, z_i)) + (0, 2/M)$$

$$= \bigcup_{i=1}^{k} ([y_i M^{-1}, (y_i + 1) M^{-1}] + M^{-1}[0, z_i + 1])$$

$$= \bigcup_{i=1}^{k} (x_i + 1/M + [0, \delta_i]) \ldots \ (B)$$
Now suppose $F \subseteq \mathbb{Z}(n)$, $|F| \leq n$. Then there is, by lemma 3, a $d$ such that
$M^{-1}F + d \subseteq E$. So

$$E + (0, 2/M) \supseteq M^{-1}F + d + (0, 2/M)$$

$$\supseteq M^{-1}F + (d, d + 1/M) + (0, 1/M)$$

$$\supseteq M^{-1}(F + c + 1) + (0, 1/M)$$

(c)

where $c = (n + 1)$. But by (B),

$$M^{-1}B + (0, 5/M) \supseteq E + 1/M + (0, 2/M)$$

$$\supseteq M^{-1}(F + c + 1) + (0, 1/M)$$

by (c).

This is equivalent to

$$M^{-1}(B + I(5)) + (0, 1/M) \supseteq M^{-1}(F + c + 1) + (0, 1/M)$$

which implies that $F + c \subseteq B + I(5) - 1$.

We take $A = B + I(5) - 1$ (mod $M$). Then

$$|(j)A^i| = n((j)M^{-1}A + (0, M^{-1}))$$

$$= n((j)(M^{-1}B + M^{-1}I(5)) + (0, M^{-1}))$$

$$< n((j)(E + (0, M^{-1}) + M^{-1}I(5))))$$

$$= n((j)E + M^{-1}(0, 5j)) < e$$, by lemma 3.

**Proof of Theorem 2.** We work in $\mathbb{Z}^n / \mathbb{Z}$ (mod $M$), for convenience. Choose $N(j, r, c/2j)$ to be the same as in Theorem 1. If $C \subseteq b(n, r)$ then, from the definition

$$C = \sum_{i=1}^{\infty} M^{-1}F_i$$

for some $F_1, F_2, \ldots \in I(N)^n$.

Write $C_i = M^{-1}(P_i + N\mathbb{Z}^n) + (0, 1)^n$. Then $C = \cap_{i=1}^\infty C_i$. Also, since $|F_i| < r$,

$$F_i \subseteq G_i^{(1)} \times \ldots \times G_i^{(n)}$$

for some $G_i^{(k)} \subseteq I(N)^n$, $|G_i^{(k)}| < r$, $1 \leq k \leq n$.

Applying Theorem 1 for each $G_i^{(k)}$, we have a $c(i^{(k)}) \in I(N)$ such that

$$G_i^{(k)} + c(i^{(k)}) \subseteq A + N\mathbb{Z}.$$

So if $c_i = c_i(F_i) = (c(i^{(1)}), \ldots, c(i^{(n)}))$,

$$F_i + c_i + N\mathbb{Z}^n \subseteq A^n + N\mathbb{Z}^n.$$

Let $d = \sum_{i=1}^{\infty} c_i M^{-1}$. Then
So, if \( B = A + \{0, 1\} \) mod \( N \), and \( K = \bigcup_{i=1}^{\infty} x_i^{-1} \), we have \( C \) and \( K \). Since \( K \) is a closed perfect self-similar Cantor set, we need only show (b). But

\[
K = \bigcap_{i=1}^{\infty} \left( N^{-1}(B + i \cdot Z^n) + N^{-1}(0, 1)^n \right)
\]

so

\[
(j) \quad K = \bigcap_{i=1}^{\infty} \left( N^{-1}((j) B + i \cdot Z^n) + N^{-1}(0, j)^n \right)
\]

\[
= \bigcap_{i=1}^{\infty} \left( N^{-1}((j) B + I(j) + i \cdot Z^n) + N^{-1}(0, 1)^n \right).
\]

Now

\[
(j) B + I(j) = (j) A + I(2j), \text{ mod } N
\]

and

\[
(j) A + I(2j) \leq 2j \| (j) A \| < \epsilon.
\]

**Proof of Theorem 3.** Again we work in \( T^n \). If \( F \subset T^n \) is any countable set, let \( x_1, x_2, \ldots \) be an enumeration of \( F \). In the notation of Theorem 1, let

\[
n_i = N(i, i, i^{-1}), \quad A_i = A(n_i) \quad \text{(so that } \| (i) A_i \| \leq i^{-1} n_i \text{)}
\]

and let

\[
M_i = n_1 \times n_2 \times \cdots \times n_i.
\]

Assuming that we have chosen \( c_k \in I(n_k)^n \), \( 0 \leq k \leq i - 1 \), we choose \( C_i \) as follows.

There is an \( F_i \subset I(n_i)^n \), \( |F_i| \leq i \) such that

\[
N_{i-1} \{ x_1, \ldots, x_i \} + Z^n \subset n_i^{-1} F_i + u_i^{-1} (0, 1)^n + Z^n
\]

(this is just a way of saying that we need at most \( i \) intervals to contain \( i \) points).

As in the proof of Theorem 2, we may choose \( c_i \) so that

\[
F_i + c_i + n_i Z^n \subset A_i^n + n_i Z^n,
\]

so

\[
\{ x_1, \ldots, x_i \} + c_i F_i^{-1} + A_i^{-1} Z^n \subset A_i^{-1} A_i^n + M_i^{-1} (0, 1)^n + M_{i-1}^{-1} Z^n
\]

For \( k \in N \), \( B \subset T^n \), \( u(k^{-1} B + k^{-1} Z^n) = u(B) \), so if

\[
c_i = M_i^{-1} A_i^n + M_{i-1}^{-1} Z^n + M_i^{-1} (0, 2)^n,
\]
and so

\[(2) \quad \mu((i) c_i) = m((i) (m_i^{-1} A_i^n + 0, 2^n)) \leq |(i) A_i^n| \times 2^n/u_i^n < 2^n/i^n.
\]

Let \(c = \sum_{i=1}^{\infty} c_i n_i^{-1}\), and suppose \(x_i\) is any member of \(F\). Then, if \(k \geq 1\),

\[
x_i + c = x_i + \sum_{j=1}^{k-1} c_j n_j^{-1} + \sum_{j=k}^{\infty} c_j n_j^{-1} + n_k^{-1} z^n
\]

\[
= x_i + c_k n_k^{-1} + n_k^{-1} z^n + \sum_{j=k+1}^{\infty} c_j n_j^{-1}
\]

\[
\subseteq \{x_1, \ldots, x_k, + c_k n_k^{-1} + n_k^{-1} z^n + k^{-1} (0, 1)^n
\]

\[
= c_k \quad \text{(from (1)).}
\]

So \(x_i + c \in \bigcap_{k=1}^{\infty} c_i^k\). If we put \(K = \bigcup_{i=1}^{\infty} \bigcap_{k=1}^{\infty} c_i^k\), \(K\) is \(F\) and \(F + c \subseteq K\).

To complete the proof by showing that, for any \(k\), \(\mu((k) K) = 0\). For suppose \(y \in (k) K\). Then \(y = y_1 + \ldots + y_k\) for some \(y_1, \ldots, y_k \in K\) for any \(z \in K\), there is a smallest \(i = i(z)\) such that \(z \in c_j^i\). Let \(n = \max(i(y_1), \ldots, i(y_k))\), then \(y \in (k) \bigcap_{j=n}^{\infty} c_j^i\). So

\[(3) \quad (k) K \subseteq \bigcup_{i=1}^{\infty} (k) \bigcap_{j=n}^{\infty} c_j^i\].

Now for any \(n\), if \(\lambda\) is any number \(\geq n\), \(k\), then

\[
m((k) \bigcap_{j=n}^{\infty} c_j^i) \leq m(c_\lambda^i) < m((i) c_\lambda^i) < (2/\lambda)^n\), from (2),
\]

so \(m((k) \bigcap_{j=n}^{\infty} c_j^i) = 0\) since \(\lambda\) was arbitrarily large.

Substituting in (3), we see that \((k) K\) is the countable union of sets of measure zero and so is of measure zero.

REFERENCES

[1] BROWN (G.) and MORAN (W.). - Raikov systems and radicals in convolution measure
[3] CONNOLLY (D. M.) and WILLIAMSON (J. H.). - Difference-covers that are not k-


