Simultaneous diophantine approximation and IP-sets

by

H. FURSTENBERG and B. WEISS (Jerusalem)

Introduction. Weyl’s theorem on equidistribution, which superseded earlier results by Hardy and Littlewood, implies that for any real polynomial \( p(t) \), and \( \varepsilon > 0 \), the diophantine inequality

\[ |p(x) - p(0) - y| < \varepsilon, \quad x \neq 0, \]

has a solution (\([9]\)). A multidimensional version (\([7]\)) tells us that we can solve

\[-|p_j(x) - p_j(0) - y_j| < \varepsilon, \quad j = 1, 2, \ldots, J, \quad x \neq 0\]

simultaneously for any finite set of real polynomials \( \{p_j(x)\} \).

In terms of the exponentials

\[ \varphi_j(n) = \exp(2\pi ip_j(n)) \]

the foregoing states that the functions \( \varphi_j \) on the integers return simultaneously arbitrarily close to their values at 0.

We shall present a general principle here according to which certain functions on \( Z \) “recur”, and the recurrence takes place along specified sets of integers, the IP-sets which we shall presently define. Because of the information on the sets of recurrence, it will follow that the functions in this class recur simultaneously. Each combination of such functions presents us with a result on diophantine approximation. Our principal result will be that if \( p_1(t_1), p_2(t_1, t_2), \ldots, p_l(t_1, t_2, \ldots, t_l) \) are arbitrary real polynomials vanishing for \( t_i = 0 \), then for any \( \varepsilon > 0 \), the system of inequalities

\[ |p_1(x_1) - x_2| < \varepsilon, \]

\[ |p_2(x_1, x_2) - x_3| < \varepsilon, \]

\[ \ldots \ldots \ldots \]

\[ |p_l(x_1, x_2, \ldots, x_l) - x_{l+1}| < \varepsilon \]

has a solution in non-zero integers.

IP-sets are closely tied up with the notion of recurrence in topological dynamics. For the background in this we refer the reader to [2], [3] and [4].
Our presentation here will avoid concepts based on dynamics; but it should be stated that dynamical notions, principally those relating to the phenomenon of distality, are not irrelevant to our discussion. Moreover, our interest in the problem stems from an application to problems of recurrence in ergodic theory (which in turn can be applied to studying which patterns necessarily occur in any subset of Z of positive density).

An IP-set in Z is a sequence \( p_1, p_2, \ldots, p_n, \ldots \) of not necessarily distinct integers together with all sums
\[
P_\sigma = p_{i_1} + p_{i_2} + \cdots + p_{i_k}, \quad i_1 < i_2 < \cdots < i_k
\]
formed by adding elements with distinct indices. To see the connection with diophantine approximation, suppose we have "recurrent" function, i.e., a bounded function \( f(n) \) on Z and some sequence \( \{g_j\} \) so that for each \( n \)
\[
f(n + g_j) \to f(n) \text{ as } j \to \infty.
\]
Now let \( \varepsilon > 0 \). For \( j_1 \) large we will have
\[
|f(g_{j_1}) - f(0)| < \varepsilon.
\]
For \( j_2 \) very large we will have
\[
|f(g_{j_1} + g_{j_2}) - f(g_{j_1})| \text{ so small that, in addition to (2) and}
\]
we will have
\[
|f(g_{j_2}) - f(0)| < \varepsilon.
\]
Proceeding inductively in this way, we can find a subsequence \( \{p_{j_1}\} = \{g_j\} \) so that for the entire IP-set \( \{p_n\} \) generated by \( \{p_{j_1}\} \)
\[
|f(p_n) - f(0)| < \varepsilon.
\]
In other words, for a recurrent function \( f(n) \), the inequality
\[
|f(n) - f(0)| < \varepsilon
\]
holds for some IP-set of \( n \). Now the functions which we will consider will have the property that for any IP-set \( S \subset \mathbb{Z} \), there exists an IP-subset \( S' \subset S \) so that (5) holds for \( n \in S' \).

To illustrate our method let us show how to prove that the system
\[
|ax - y| < \varepsilon,
\]
\[
|bx - z| < \varepsilon
\]
has a non-trivial solution. (This particular case of (1) can also be deduced directly from the minimality of a certain 3-dimensional "nilflow". See [11].)

Let \( I(x) = \lfloor x + \frac{1}{2} \rfloor \) denote the integer nearest \( x \). We will show in the sequel that the functions \( \exp(2\pi i an) \) and \( \exp(2\pi i \beta n (x n)) \) are both in the class of "IP-recurrent" functions having the property described above. If \( S \) is an IP-set on which \( \exp(2\pi i an) \) is close to 1, then with \( x \in S \) and \( y = I(ax) \) we have a solution to the first inequality of (6). But now our second function \( \exp(2\pi i \beta n (x n)) \) comes arbitrarily close to 1 for \( n \) restricted to \( S \), and so the second inequality is obtained as well. Since moreover the values of \( n \) for which \( x = n, y = I(x) \), \( z = I(\beta n (x n)) \) form a solution to (6) themselves fill an IP-set \( S' \subset S \) we could proceed to obtain further inequalities.

Thus the main part of our exposition is devoted to obtaining a wide class of IP-recurrent functions. For each polynomial \( p(t) \) the function \( \exp(2\pi i p(n)) \) will be seen to be IP-recurrent. We will repeatedly use the fact that IP-recurrent functions form an algebra.

We expect that IP-recurrence is a rather special property representing the exception, rather than the rule. For example, for almost all \( x \)
\[
\exp(2\pi \sin \cos n x)
\]
is not IP-recurrent, as we shall prove in Section 6. We do not know however whether there is an \( \alpha \) for which
\[
|\exp(2\pi \sin \cos n x) - 1| < \varepsilon
\]
fails to have a solution.

One reason for the usefulness of IP-recurrent functions is that not only does the inequality
\[
|f(n) - f(0)| < \varepsilon
\]
have a non-zero solution \( n \), but the set of solutions forms a relatively dense (syndetic) set: that is, the solutions for \( n > 0 \) can be arranged as
\[
0 < n_1 < n_2 < \cdots < n_k < \cdots
\]
with \( n_{k+1} - n_k \) bounded, and similarly for \( n < 0 \). In particular, the set of solutions has positive lower density.

1. Hindman's Theorem and its refinements. We begin with the following Ramsey-type theorem. We denote by \( \mathcal{F} \) the family of all finite subsets of the natural numbers.

**Theorem 1** (N. Hindman ([5] and [6])). If \( \mathcal{F} \) is partitioned into finitely many sets, \( \mathcal{F} = C_1 \cup C_2 \cup \ldots \cup C_l \), then there exists a sequence of disjoint sets \( \sigma_1, \sigma_2, \ldots, \sigma_n \) so that for some \( j \), all finite unions \( \sigma_{i_1} \cup \sigma_{i_2} \cup \ldots \cup \sigma_{i_k} \) belong to the same \( C_j \).

For any finite partition of the natural numbers \( N = D_1 \cup D_2 \cup \ldots \cup D_l \), let us derive a partition of \( \mathcal{F} \) by setting
\[
\sigma = \{i_1, i_2, \ldots, i_k\} \in C_j \iff \sum_{i \in \sigma} 2^i \in D_j.
\]
Hindman's theorem then gives the following far reaching extension of Schur's lemma:

**Theorem 2.** If $N = D_1 \cup D_2 \cup \ldots \cup D_n$, then for some $j$, $D_j$ contains an IP-set.

If $S$ is an IP-set, it is generated by a sequence $\{p_i\}$ and each element of $S$ has the form $p_\sigma = \sum_{i \in \sigma} p_i$, where $\sigma \in \mathcal{F}$.

Suppose we partition an IP-set $\{p_\sigma\}$. This induces a partition of $\mathcal{F}$ and by Theorem 1 we can find $\tau_1, \tau_2, \ldots, \tau_n$ so that all $\tau_1 \cup \tau_2 \cup \ldots \cup \tau_k$ belong to the same set. The subset of the form

$$P_\sigma = P_{\tau_1} \cup \ldots \cup P_{\tau_k}$$

again forms an IP-set all of whose terms belong to the same cell of the partition of $\{p_{\sigma}\}$. Thus we have the following extension of Theorem 2.

**Theorem 3.** If $S = \{p_\sigma\}$ is any IP-set and $S = C_1 \cup C_2 \cup \ldots \cup C_k$ is a partition, then for some $j$, $C_j$ contains an IP-subset of $S$.

The next result shows the relevance of IP-sets for diophantine approximation.

**Theorem 4.** If $\{p_\sigma\}$ is any IP-set and $x$ a real number then for $\varepsilon > 0$ the inequality $|e^{2\pi i p_\sigma x} - 1| < \varepsilon$ has a solution for some $\sigma \in \mathcal{F}$.

**Proof.** Divide the unit circle into small arcs $A_j$, and set

$$p_\sigma \in A_j \iff e^{2\pi i p_\sigma x} \in A_j.$$

By Theorem 3, for some $\sigma$, $p_{\tau k}$, $p_a$, and $p_{\tau k}$ belong to the same $C_j$. So

$$\xi_\sigma = \exp(2\pi i p_{\tau k} x), \quad \xi_a = \exp(2\pi i p_a x) \quad \text{and} \quad \xi_\tau = \xi,$$

all belong to the same arc. If the arcs are small this implies $|\xi_\tau - 1| < \varepsilon$ which proves the theorem.

In fact the argument shows that $|\exp(2\pi i n x) - 1| < \varepsilon$ has a solution for $n$ along an entire IP-subset of $S$.

In general, we refer to a sequence of elements of any set $\{x_\sigma\} \subseteq X$ indexed by $\sigma \in \mathcal{F}$ as an $\mathcal{F}$-sequence. We can form $\mathcal{F}$-subsequences of an $\mathcal{F}$-sequence as follows: Let $\tau_1, \tau_2, \ldots$ be disjoint sets in $\mathcal{F}$. If

$$x_\tau = \bigcup_{\tau_k \in \tau} x_\tau_k$$

then $\{x_\tau\}$ is an $\mathcal{F}$-subsequence of $\{x_\sigma\}$. Notice that an $\mathcal{F}$-subsequence of an IP-set in $Z$ is again an IP-set. Also notice that an $\mathcal{F}$-subsequence of an $\mathcal{F}$-subsequence is an $\mathcal{F}$-subsequence.

Now suppose $X$ is a metric space, and let $\{x_{\sigma}\}$ be an $\mathcal{F}$-sequence in $X$. We shall say

$$\mathcal{F}\text{-lim}_x x_\sigma = x \in X \quad \text{or} \quad x_\sigma \to x$$

if, for any $\varepsilon > 0$, there exists $\sigma(\varepsilon)$ such that whenever $\sigma \cap \sigma(\varepsilon) = \emptyset$ (i.e., $\sigma$ is based on indices sufficiently far out),

$$d(x_\sigma, x) < \varepsilon.$$

It is now not difficult to deduce from Theorem 1 the following:

**Theorem 5.** If $X$ is a compact metric space, then any $\mathcal{F}$-sequence in $X$ has a convergent $\mathcal{F}$-subsequence.

2. IP-recurrence.

**Definition.** A function $f(n)$ on $Z$ with values in a compact metric space is IP-recurrent ($f \in \text{IPR}$ or $f$ is IPR) if for any IP-set $\{p_\sigma\}$ there exists an $\mathcal{F}$-subsequence $\{p_{\sigma}^\prime\}$ so that

$$\mathcal{F}\text{-lim}_\sigma f(n + p_\sigma) = f(n)$$

for every $n$.

The following is easily proved.

**Theorem 6.** If $\xi(n)$ is IPR with values in $X$ and $\eta(n)$ is IPR with values in $Y$ then $(\xi(n), \eta(n))$ is IPR with values in $X \times Y$.

If $\mathcal{F}$ denotes the family of bounded, complex-valued functions on $Z$ that are IP-recurrent, then $\mathcal{F}$ is an algebra closed under passage to uniform limits.

The crucial property for us is the following:

**Corollary.** If $\xi_1(n), \xi_2(n), \ldots, \xi_k(n)$ are IPR functions, then for any $\varepsilon > 0$ we can find $n > 0$ with

$$|\xi_1(n) - \xi_1(0)| < \varepsilon, \quad |\xi_2(n) - \xi_2(0)| < \varepsilon, \quad \ldots, \quad |\xi_k(n) - \xi_k(0)| < \varepsilon.$$

The next result plays the role of the van der Corput lemma in equidistribution theory.

**Theorem 7.** Let $f(n)$ be an IPR function with values in the unit circle of $C$. If $g(n)$ satisfies $g(n+1)g(n)^{-1} = f(n)$, then $g(n)$ is an IPR function.

**Proof.** Let $\{p_\sigma\}$ be an IP-set of integers. We may assume that we have already passed to a subsequence for which

$$\mathcal{F}\text{-lim}_\sigma f(n + p_\sigma) = f(n)$$

and moreover such that $\mathcal{F}\text{-lim}_\sigma g(n + p_\sigma)$ exists for all $n$. Here we have used Theorem 5 and the compactness of the infinite dimensional torus. Set

$$g'(n) = \mathcal{F}\text{-lim}_\sigma g(n + p_\sigma).$$
Then

\[ g'(n+1)g'(n)^{-1} = \lim_{n \to \infty} g(n+1+p_0)g(n+p_0)^{-1} \]

\[ = \lim_{n \to \infty} f(n+p_0) = f(n) \]

\[ = g(n+1)g(n)^{-1}. \]

It follows that there exists a constant \( \gamma \) so that \( g'(n) = \gamma g(n) \), and we have

\[ \lim_{n \to \infty} g(n+p_0) = \gamma g(n). \]

For some \( \sigma_0 \), if \( \sigma \cap \sigma_0 = \emptyset \), we will have

\[ |g(p_0) - \gamma g(0)| < \varepsilon. \]

For some \( \tau \cap \sigma_0 = \emptyset \) and \( \tau \cap \sigma = \emptyset \) we will have

\[ |g(p_0) - \gamma g(0)| < \varepsilon. \]

For some \( \sigma_1 \), if \( \sigma \cap \sigma_1 = \emptyset \), we will have, in addition,

\[ |g(p_0+p_1) - \gamma g(0)| < \varepsilon. \]

Since \( \{p_0\} \) is an IPR-set, \( p_0+p_1 \). Then we have

\[ |g(p_0+p_1) - \gamma^2 g(0)| < 2\varepsilon, \quad |g(p_0+p_1) - \gamma g(0)| < \varepsilon. \]

Since \( \varepsilon > 0 \) is arbitrary we deduce that \( \gamma = 1 \) and this proves the theorem. \( \blacksquare \)

Another result which enables us to manufacture IPR functions is the following.

**Theorem 8.** Let \( f(n) \) be an \( X \)-valued IPR function and let \( \varphi : X \to Y \) be a function continuous at the points \( f(n) \in X \). Then \( g(n) = \varphi(f(n)) \) is an IPR-function.

The proof is immediate.

By Theorem 7, since the constant function is IPR, we deduce that \( \exp(2\pi i \lambda x) \) is IPR. Proceeding inductively we find that \( \exp(2\pi i p(n)) \) is IPR for any polynomial \( p(n) \).

3. Extending the family of IPR functions.

**Definition.** We will say that a real valued function \( f(n) \) is LIPR if for all real \( \lambda \), \( \exp(2\pi i \lambda f(n)) \) is IPR.

Thus all polynomials are LIPR. Also all IPR functions are LIPR as well (by Theorem 8). We shall see in Section 6 that for some \( \alpha \), \( f(n) = n \cos n \alpha \) is not LIPR. This shows that the family LIPR is not closed under multiplication. In this section we shall construct an algebra of functions in LIPR extending the polynomials.

**Lemma 9.** Let \( g(n) \) be an IPR function with finite range and let \( f \in \text{LIPR} \). Then the function \( g(n)f(n) \) is in LIPR.

**Proof.** Let \( \{t_1, t_2, \ldots, t_I\} \) be the range of \( g \). We can find polynomials \( p_i(t), i = 1, 2, \ldots, I \), such that \( p_i(t_j) = \delta_{ij} \). Then one has

\[ \exp(2\pi i \lambda \delta_{ij} g(n)f(n)) = \sum_{i=p_i} \exp(2\pi i \lambda f(n)) = \exp(2\pi i \lambda f(n)) \]

But the right-hand side of (12) is the sum of products of functions in IPR and so it is in itself in IPR. This proves the lemma. \( \blacksquare \)

The set of functions LIPR is translation invariant, since IPR is, and it is closed under addition, since IPR is closed under multiplication. The set of finite valued functions in IPR form a ring which we denote by \( \mathcal{R} \) and LIPR is a module under multiplication by \( \mathcal{R} \).

We denote by \( \Delta F \) the function \( \Delta F(n) = F(n+1) - F(n) \). Then Theorem 7 tells us that \( \Delta F \in \text{LIPR} \) implies that \( F \in \text{LIPR} \). Now let us define a space of function as follows.

**Definition.** \( \mathcal{L} \) denotes the smallest space of functions on \( Z \) satisfying

(i) the constants are in \( \mathcal{L} \),

(ii) \( \mathcal{L} \) is a module under multiplication by \( \mathcal{R} \),

(iii) if \( \Delta F \in \mathcal{L} \), then \( F \in \mathcal{L} \).

Since the intersection of spaces \( \mathcal{L}_K \) with these properties again has these properties, \( \mathcal{L} \) is well defined. If \( T \) denotes translation, then \( T \mathcal{L} \) has these properties, and so by minimality \( T \mathcal{L} = \mathcal{L} \) so that \( \mathcal{L} \) is translation invariant. We will see that \( \mathcal{L} \) is closed under multiplication.

In any case we have

**Theorem 10.** \( \mathcal{L} = \text{LIPR} \).

**Proof.** We verify by Theorem 7 and Lemma 9 that \( \text{LIPR} \) has properties (i), (ii), and (iii). \( \blacksquare \)

Consider the following subspaces of \( \mathcal{L} \). We take \( \mathcal{L}_0 = \mathcal{R} \). Proceed inductively to define spaces \( \mathcal{L}_n \) and \( \mathcal{L}_n' \) by the following:

(i) If \( \Delta F \in \mathcal{L}_{n-1} \) then \( F \in \mathcal{L}_n \).

(ii) If \( F \in \mathcal{L}_n' \) and \( g \in \mathcal{R}, j = 1, 2, \ldots, J \) then \( \sum_{j=1}^J f_j g_j \in \mathcal{L}_n' \).

**Lemma 11.** Each of the spaces \( \mathcal{L}_n \) is translation invariant and \( \mathcal{L}_n \subset \mathcal{L}_{n+1} \).

**Proof.** Both statements are proved by induction. Translation invariance passes from \( \mathcal{L}_0 \) to \( \mathcal{L}_1 \) to \( \mathcal{L}_2 \) to \( \mathcal{L}_2 \) etc.

The second statement is true for \( \mu + \nu = 0 \). Suppose it is true for \( \mu' + \nu' < \mu + \nu \). Suppose \( F \in \mathcal{L}_n, g \in \mathcal{R} \). Then

\[ \Delta g_F(n) = f(n+1)g(n+1) - f(n)g(n) = \Delta f(n)g(n+1) + f(n)g'(n), \]

so

\[ \Delta g_F \in \mathcal{L}_{n-1} \mathcal{L}_n + \mathcal{L}_n \mathcal{L}_n' \subset \mathcal{L}_{n+1} \mathcal{L}_{n+1} = \mathcal{L}_{n+1} \mathcal{L}_{n+1} \]

and \( g_F \in \mathcal{L}_{n+1} \subset \mathcal{L}_{n+1} \).
To check the product of elements in $L_\alpha$ and $L_\nu$ it suffices to consider $(h_1 f) (h_2 g)$ with $h_1, h_2 \in \mathbb{R}, f \in L_\alpha, g \in L_\nu$; but this case follows immediately.

**Theorem 12.** The space $L$ is the union of $L_\nu$ and forms an algebra.

**Proof.** Since $\bigcup L_\nu$ has the properties of the definition of $L$ we must have $L = \bigcup L_\nu$.

Clearly $L$ contains all polynomials. An example of a non-polynomial function in $L_1$ is

$$g(n) = \left[2n + \frac{1}{2}\right]$$

where $\alpha$ is irrational. To see this note that

$$l(x) = \left[x + \alpha + \frac{1}{2}\right] - \left[x + \frac{1}{2}\right]$$

is a periodic function of $x$ with discontinuities when

$$x \equiv \frac{1}{2}, \frac{1}{2} - \alpha \pmod{1}.$$ 

So $l(x) = L(\exp(2\pi i x))$ with $L(z)$ continuous except for $z = -1, \ldots, -e^{2\pi i \alpha}$. Hence by Theorem 8, $L(\exp(2\pi i x))$ is IPR. But

$$L(\exp(2\pi i n x)) = l(nx) = g(n + 1) - g(n)$$

and since $l(nx)$ is in $L_\alpha$, we have $g \in L_\alpha$.

We construct systematically a subfamily of $L$ which will be useful for problems in diophantine approximation.

Let $h_\alpha(x) = x - \lfloor x - \alpha \rfloor$.

**Lemma 13.** For all $x, y$

$$h_\alpha(x) - h_\alpha(y) = h_\alpha(x - y) + G_\alpha(\exp(2\pi i x), \exp(2\pi i y))$$

where $G_\alpha(z, w)$ is a bounded integer valued function on the torus continuous along the curves $z = e^{2\pi i k}, w = e^{2\pi i k}, z = e^{2\pi i k}$.

**Proof.** Since $h_\alpha(x + 1) = h_\alpha(x), G_\alpha$ defined by (13) is a function on the torus and it can be discontinuous only if either $h_\alpha(x), h_\alpha(y)$ or $h_\alpha(x - y)$ is discontinuous. Since $h_\alpha(x) \equiv x (\text{mod} 1)$ it follows that $G_\alpha$ is integer valued and it is bounded since $h_\alpha$ is bounded.

We now prove

**Proposition 14.** For each function $f \in L$ there is a countable set $\Theta(f) \subset \mathbb{R}$ such that if $0 \notin \Theta(f)$ then $h_\alpha(f(n))$ is a function in $L$.

**Proof.** We prove this for $f \in L_\alpha$, by induction on $v$. For $f \in L_0, f(n)$ is finite valued and IPR. For all but countably many values of $\theta$, $h_\alpha$ is continuous on the range of $f(n)$. By Theorem 8, $h_\alpha(f(n))$ is again IPR, and so $h_\alpha f \in L_\alpha$. Assume the proposition valid for functions in $L_{\alpha-1}$, then $\Delta f \in L_{\alpha-1}$. Consider now $h_\alpha f$. We have by Lemma 13,

$$h_\alpha f(n + 1) - h_\alpha f(n) = h_\alpha(\Delta f(n)) + G_\alpha(\exp 2\pi i (n + 1), \exp 2\pi i f(n)).$$

Hence if $\theta \notin \Theta(\Delta f) \cup \bigcup f(n) + Z$, the function to the right of (14) is in $L_\alpha$, since $\exp 2\pi i f(n)$ is in IPR and $G_\alpha$ is continuous at the points under consideration.

Next suppose $f = \sum g_j f_j$ where $f_j \in L_\nu$ and $g_j \in \mathbb{R}$. Let the range of $g_j$ be $[t_{j1}, t_{j2}, \ldots, t_{j\nu}]$. We find polynomials $p_{j\nu}, 1 \leq q \leq j$ so that

$$p_{j\nu}(t_{j\nu}) = \delta_{q\nu}.$$ 

We now check that

$$h_\alpha f(n) = h_\alpha(\sum g_j f_j(n)) = \sum_{r_{j1}, \ldots, r_{j\nu}} p_{r_{j1}}(g_1(n)) \cdots p_{r_{j\nu}}(g_\nu(n)) h_\alpha(\sum_{j=1}^j t_{r_{j1}} f_1(n)).$$

Since $\sum_{j=1}^j t_{r_{j1}} f_j \in L_\nu$, the function $h_\alpha(\sum_{j=1}^j t_{r_{j1}} f_j(n))$ will be in $L_\nu$ provided $\theta$ avoids the countable set $\Theta(\sum_{j=1}^j t_{r_{j1}} f_j(n))$. Moreover each $p_{r_{j\nu}}(g_j(n))$ is in $L_\nu = \mathbb{R}$. Hence we may take

$$\Theta(f) = \bigcup_{r_{j1}, \ldots, r_{j\nu}} \Theta(\sum_{j=1}^j t_{r_{j1}} f_j(n))$$

and for $\theta \notin \Theta(f)$, $h_\alpha f \in L_\alpha$.

**4. Applications to diophantine approximation.** Let

$$I_\theta(x) = x - h_\alpha(x) = [x - \theta].$$

**Proposition 14'.** Let $f_1(n), f_2(n), \ldots, f_{\nu}(n)$ be functions in $L$. Then if $\theta \notin \Theta(f)$ and $p(x_1, x_2, \ldots, x_{\nu})$ is any real polynomial, the function

$$f(n) = p(f_1(n), f_2(n), \ldots, f_{\nu-1}(n), I_\theta(f_{\nu}(n)))$$

is in $L_\nu$.

**Proof.** We can write $f(n) = p'(f_1(n), f_2(n), \ldots, f_{\nu-1}(n), f_\nu(n), h_\alpha f_{\nu}(n))$ for some other polynomial $p'$. Since $L_\nu$ is an algebra and each of the functions in question is in $L_\nu$ so is $f$.

Now suppose we have a solution to an inequality of the form

$$|p(x_1, x_2, \ldots, x_{\nu}) - y| < \epsilon$$
LEMMA 16. If $S \subseteq \mathbb{Z}$ is not relatively dense, there is an IP-set $\{p_n\}$ in $\mathbb{Z}$ which does not meet $S$.

Proof. For every $n$ there are intervals $(a_n, a_n + n) \subseteq \mathbb{Z} \setminus S$. Choose $p_n \in \mathbb{Z} \setminus S$. Choosing an interval of length $|p_n|$ outside of $S$ we find $p_n \notin S$ with $p_1 \neq S$. Continue inductively so that after $p_1, p_2, \ldots, p_4$ have been found so that no partial sum is in $S$, find an interval outside of $S$ of length $\geq 2|p_1| + |p_2| + \ldots + |p_4| + 1$. If $p_5 + p_2 + \ldots + p_4 + p_5 \notin S$ for $i_1 < i_2 < \ldots < i_4 < l+1$. This proves the lemma.

Now let $f(n)$ be an IPR function with values in a compact metric space. Then for any IP-set $\{p_n\}$ and for any $\varepsilon > 0$ we will have

$$d(f(p_n), 0) < \varepsilon$$

for some $p_n$. Consider the set $S$ of $n$ for which $d(f(n), 0) < \varepsilon$. If this set were not relatively dense, use the lemma to find an IP-set in the complement of $S$. This contradicts the definition of IP recurrence we must have recurrence along a relatively dense set. Applying this to a vector valued function $(f_1(n), \ldots, f_l(n))$ we obtain the following.

THEOREM 17. If $f_1(n), f_2(n), \ldots, f_l(n)$ are real or complex-valued IPR functions then for any $\varepsilon > 0$, the set of $n$ simultaneously satisfying

$$|f_1(n) - f_1(0)| < \varepsilon, \quad |f_2(n) - f_2(0)| < \varepsilon, \quad \ldots, \quad |f_l(n) - f_l(0)| < \varepsilon$$

is relatively dense.

6. The function $n \cos \pi z$. It is not always easy to ascertain if a function is IPR. We prove in this section

THEOREM 18. For almost all $t$, the function $f(n) = n \cos \pi z$ is not in LIPR, and $\exp(2\pi \cos \pi z)$ is not in IPR.

This proves that LIPR is not closed under multiplication.

Let $T^\mathbb{Z}$ denote the space of sequences $\{x_n\}_{n \in \mathbb{Z}}$ with the product topology. We denote by $\sigma$ the shift on $T^\mathbb{Z}$: $(x_n)_n = x_{n+1}$. We define the positive orbit of a point $x \in T^\mathbb{Z}$ as the set $\{\sigma^n x\}_n \subseteq T^\mathbb{Z}$ and the positive orbit closure of $x$ is the closure of this set.

Theorem 18 will follow from the next proposition.

PROPOSITION 19. For almost all $t$ the positive orbit closure of the point $c(t) = e^{i\pi \cos \pi t}$ is all of $T^\mathbb{Z}$.

Assume this has been established and let $x$ satisfy the statement of the proposition. In particular the point with all coordinates $-1$ in the orbit closure of $c(t)$. Now this means that there are arbitrarily long intervals of $n$ with

$$e^{i\pi \cos \pi (n+1)} < \sqrt{2}$$
and 

$$|e^{2\pi n \text{const}} - 1| > \sqrt{2}.$$ 

By Theorem 17, $e^{2\pi n \text{const}}$ cannot be IPR.

We proceed to prove the proposition.

We shall check that for $n_k$ growing sufficiently rapidly, for any $d$ the sequence

$$\left( e^{2\pi i(n_k + 1) \text{const}(n_k + 1)t}, \ldots, e^{2\pi i(n_k + d - 1) \text{const}(n_k + d - 1)t} \right)$$

is equidistributed on the $d$-torus for a.e. $t$. In particular it will follow that the positive orbit closure is all of $T^d$. LeVeque ([3]) has shown that for a.e. $t$, $e^{2\pi n \text{const}t}$ is itself equidistributed on $T$. It is quite reasonable to suppose that we could take $n_k = k$ even in our multi-dimensional case. However, since that is not the main point of this illustration we shall not pursue that more delicate question. To prove the theorem we use H. Weyl's criterion and a standard elaboration of his proof that for any sequence of integers going to infinity the fractional part of $[n_k t]$ is equidistributed in $[0, 1]$ for a.e. $t$, to reduce the problem to the following lemma:

**Lemma 20.** For any integers $a_j$, $0 \leq j < d$ not all zero and any fixed $m$ we have

$$\lim_{n \to \infty} \int_0^{2\pi} \left| \sum_{j=0}^{d-1} (n+j)a_j \cos(n+j)t - \sum_{j=0}^{d-1} (m+j)a_j \cos(m+j)t \right| dt = 0.$$ 

Since the arguments are fairly routine we will only sketch the proofs briefly.

**Proof.** Denote for brevity

$$f_n(t) = \sum_{j=0}^{d-1} (n+j)a_j \cos(n+j)t.$$ 

Clearly $f_n(t) - f'_n(t)$ has at most $O(n)$ zeros in $[0, 2\pi]$, and the same is true for $f'_n - f''_n$. On each interval of monotonicity of $f'_n - f''_n$ we look at a subinterval $(a, b)$ where this derivative has a value at least $n^{1/2}$. The standard estimates show that our integral evaluated over such an interval $(a, b)$ is $O(1/n^{1/2})$ so that the total contribution of such intervals is $O(1/n^{1/2})$. Next we show that the measure of $[0, 2\pi]$ not covered by such intervals tends to zero as $n \to \infty$. Indeed since

$$f'_n(t) = \sum_{j=0}^{d-1} (n+j)a_j \sin(n+j)t$$

and $m$ is fixed, $|f'_n(t) - f''_n(t)| < n^{3/2}$ forces

$$\sum_{j=0}^{d-1} \left(1 + \frac{j}{n}\right)^2 \frac{a_j \sin(n+j)t}{n} = O(1/n^{1/2}).$$

However we can write this latter expression as

$$I_m \left( \sum_{j=0}^{d-1} \left(1 + \frac{j}{n}\right)^2 a_j \frac{e^{jn}}{n} \right) = I_m \left( e^{jn} Q_n(t) \right)$$

where $Q_n(t)$ converges uniformly to a non zero polynomial of degree at most $d-1$. From this it easily follows that means $|t| \sum_{j=0}^{d-1} (n+j)a_j \cos(n+j)t| \to 0$ as $n \to \infty$ which completes the proof.

**Proof of Proposition 19.** Using the lemma and a diagonalization procedure we choose a sequence $n_k \to \infty$ such that for any fixed $d$ and choice of $(a_0, a_1, \ldots, a_{d-1})$ there is a $k_0 = k(d, a_0, \ldots, a_{d-1})$ such that for all $k_0 \leq k < l$ one has

$$\sum_{j=0}^{d-1} (n+j)a_j \cos(n+j)t - \sum_{j=0}^{d-1} (n_j+j)a_j \cos(n_j+j)t dt < 2^{-k}.$$ 

It follows that

$$\frac{1}{N} \sum_{k=1}^{N} \left| \sum_{j=0}^{d-1} (n+j)a_j \cos(n+j)t \right|^2 dt = O(1/N)$$

and thus

$$\sum_{N=1}^{\infty} \frac{1}{N^2} \sum_{k=1}^{\infty} \left| \sum_{j=0}^{d-1} (n+j)a_j \cos(n+j)t \right|^2 dt < \infty.$$ 

Now for a set of full measure of $t$'s we deduce that

$$g_n^2 = \frac{1}{N^2} \sum_{k=1}^{\infty} \left| \sum_{j=0}^{d-1} (n+j)a_j \cos(n+j)t \right|^2 \to 0$$

whence it follows, since the exponentials are bounded, that $g_n(t) \to 0$ as $N \to \infty$ not necessarily along squares. Then Weyl's criterion gives the equidistribution.

**References**


Large deviations of sums of independent random variables

by

HUGH L. MONTGOMERY* (Ann Arbor, Mich.) and ANDREW M. ODLYZKO (Murray Hill, N.J.)

Dedicated to Pál Erdős on the occasion of his 75-th birthday

1. Statement of results. Our object is to estimate the probability that a sum of independent random variables is large. In this direction we derive a rather precise upper bound, and a corresponding lower bound.

Theorem 1. Let \( X_1, X_2, \ldots \) be independent random variables such that\( P(X_n = 1) = 1/2, \ P(X_n = -1) = 1/2 \). Let \( \{r_n\} \) be a non-increasing sequence of non-negative real numbers for which

\[
\sigma^2 = \sum_{n=1}^{\infty} r_n^2 < \infty,
\]

and put \( X = \sum_{n=1}^{\infty} r_nX_n \). If \( N \) and \( V \) are chosen so that \( \sum_{n \leq N} r_n \leq V/2 \), then

\[
P(X \geq V) \leq \exp\left(-\frac{1}{8} V^2 \left( \sum_{n \leq N} r_n^2 \right)^{-1}\right).
\]

If \( \sum_{n \leq N} r_n \geq 2V \) then

\[
P(X \geq V) \geq 2^{-2V} \exp\left(-120V^2 \left( \sum_{n \geq N} r_n^2 \right)^{-1}\right).
\]

Also, if \( \sum_{n \leq N} r_n \geq V \) then

\[
P(X \geq V) \geq 2^{-N-1}.
\]

* Research supported in part by National Science Foundation Grant NSF DMS 85-02804.