References

[1] L. Alaoglu and P. Erdős, *On highly composite and similar numbers*, Trans. Amer. Math. Soc. 56 (1944), p. 448–469.
[2] G. Bessi et J. L. Nicolas, *Nombres 2-hautement composés*, J. Math. pures et appl. 56 (1977), p. 307–326.
[3] P. Erdős, *On highly composite numbers*, J. London Math. Soc. 19 (1944), p. 130–133.
[4] P. Erdős et J. L. Nicolas, *Répartition des nombres superabondants*, Bull. Soc. Math. France 103 (1975), p. 65–90.
[5] D. R. Heath-Brown and H. Iwaniec, *On the difference between consecutive primes*, Inv. Math. 55 (1979), p. 49–69.
[6] D. W. Masser and P. Shiu, *On sparsely totient numbers*, Pacific J. Math. 121 (1986), p. 407–426.
[7] H. L. Montgomery and R. C. Vaughan, *The large sieve*, Mathematika 20 (1973), p. 119–134.
[8] J. L. Nicolas, *Ordre maximal d'un élément du groupe des permutations et highly composite numbers*, Bull. Soc. Math. France 97 (1969), p. 129–191.
[9] — *Répartition des nombres hautement composés de Ramanujan*, Canad. J. Math. 23 (1971), p. 116–130.
[10] — *Répartition des nombres largement composés*, Acta Arith. 34 (1980), p. 379–390.
[11] — *Sur les entiers n pour lesquels il y a beaucoup de groupes abéliens d'ordre n*, Annales Inst. Fourier 28 (1978), p. 1–16.
[12] S. Pillaï, *Highly abundant number*, Bull. Calcutta math. Soc. 35 (1943), p. 141–156.
[13] — *Highly composite numbers of the t^{th} order*, J. Indian Math. Soc. 8 (1944), p. 61–74.
[14] S. Ramanujan, *Collected papers*, University Press, Cambridge 1927.
[15] G. Robin, *Méthodes d'optimisation pour un problème de théorie des nombres*, R.A.I.R.O. Informatique théorique 17 (1983), p. 239–247.
[16] — *Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann*, J. Math. pures et appl. 63 (1984), p. 187–213.
[17] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), p. 64–94.
[18] N. Slater, *Gaps and steps for the sequence $n\theta$ mod 1*, Proc. Cambridge Phil. Soc. 63 (1967), p. 1115–1123.
[19] T. H. Tran, *Nombres hautement composés de Ramanujan généralisés*, C. R. Acad. Sci. Paris, Ser. A–B, 282 (1976), p. 939–942.
[20] M. Waldschmidt, *A lower bound for linear forms in logarithms*, Acta Arith. 37 (1980), p. 257–283.

DÉPARTEMENT DE MATHÉMATIQUES
UNIVERSITÉ DE LIMOGES
123 Avenue A. Thomas
F-87060 Limoges Cédex
France

Reçu le 13.6.1986 (1650)

ACTA ARITHMETICA
XLIX (1988)

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

$$\varphi_j(n) = \exp(2\pi i p_j(n))$$

the foregoing states that the functions φ_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 $\boldsymbol{Z}$ "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

$$(1) \qquad \begin{aligned} |p_1(x_1)-x_2| &< \varepsilon, \\ |p_2(x_1, x_2)-x_3| &< \varepsilon, \\ &\ldots\ldots\ldots\ldots \\ |p_l(x_1, x_2, \ldots, x_l)-x_{l+1}| &< \varepsilon \end{aligned}$$

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 $\mathbf{Z}$ of positive density).

An *IP-set* in $\mathbf{Z}$ is a sequence $p_1, p_2, \ldots, p_n, \ldots$ of not necessarily distinct integers together with all sums

$$p_\sigma = p_{i_1 i_2 \ldots i_k} = p_{i_1} + p_{i_2} + \ldots + p_{i_k}, \quad i_1 < i_2 < \ldots < i_k$$

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 $\mathbf{Z}$ and some sequence $\{g_j\}$ so that for each n, $f(n+g_j) \to f(n)$ as $j \to \infty$.

Now let $\varepsilon > 0$. For j_1 large we will have

$$|f(g_{j_1}) - f(0)| < \varepsilon. \tag{2}$$

For j_2 very large we will have $|f(g_{j_1}+g_{j_2}) - f(g_{j_1})|$ so small that, in addition to (2) and

$$|f(g_{j_2}) - f(0)| < \varepsilon, \tag{3}$$

we will have

$$|f(g_{j_1}+g_{j_2}) - f(0)| < \varepsilon. \tag{4}$$

Proceeding inductively in this way, we can find a subsequence $\{p_i\} = \{g_{j_i}\}$ so that for the entire IP-set $\{p_\sigma\}$ generated by $\{p_i\}$

$$|f(p_\sigma) - f(0)| < \varepsilon.$$

In other words, for a recurrent function $f(n)$, the inequality

$$|f(n) - f(0)| < \varepsilon \tag{5}$$

holds for *some* IP-set of n. Now the functions which we will consider will have the property that for *any* IP-set $S \subset \mathbf{Z}$, 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

$$\begin{aligned} |\alpha x - y| &< \varepsilon, \\ |\beta x y - z| &< \varepsilon \end{aligned} \tag{6}$$

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 [1].)

Let $I(x) = [x+\frac{1}{2}]$ denote the integer nearest x. We will show in the sequel that the functions $\exp(2\pi i\alpha n)$ and $\exp(2\pi i\beta n I(\alpha n))$ are both in the class of "IP-recurrent" functions having the property described above. If S is an IP-set on which $\exp(2\pi i\alpha n)$ is close to 1, then with $x \in S$ and $y = I(\alpha x)$ we have a solution to the first inequality of (6). But now our second function $\exp(2\pi i\beta n I(\alpha n))$ comes arbitrarily close to 1 for n restricted to S, and so the second inequality is obtained as well. Since moveover the values of n for which $x = n$, $y = I(\alpha n)$, $z = I(\beta n I(\alpha n))$ 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 α

$$\exp(2\pi i n \cos n\alpha)$$

is not IP-recurrent, as we shall prove in Section 6. We do not know however whether there is an α for which

$$|\exp(2\pi i n \cos n\alpha) - 1| < \varepsilon$$

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

$$0 < n_1 < n_2 < \ldots < n_k < \ldots$$

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 $\mathscr{F}$ the family of all finite subsets of the natural numbers.

THEOREM 1 (N. Hindman ([5] and [6])). *If $\mathscr{F}$ is partitioned into finitely many sets, $\mathscr{F} = C_1 \cup C_2 \cup \ldots \cup C_l$, then there exists a sequence of disjoint sets $\sigma_1, \sigma_2, \ldots, \sigma_n, \ldots$ 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 $\mathbf{N} = D_1 \cup D_2 \cup \ldots \cup D_l$, let us derive a partition of $\mathscr{F}$ by setting

$$\sigma = \{i_1, i_2, \ldots, i_k\} \in C_j \Leftrightarrow \sum_{i \in \sigma} 2^i \in D_j.$$

Hindman's theorem then gives the following far reaching extension of Schur's lemma:

THEOREM 2. *If $N = D_1 \cup D_2 \cup \ldots \cup D_l$, 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 $\sigma \in \mathscr{F}$.

Suppose we partition an IP-set $\{p_\sigma\}$. This induces a partition of $\mathscr{F}$ and by Theorem 1 we can find $\tau_1, \tau_2, \ldots, \tau_n, \ldots$ so that all $\tau_{i_1} \cup \tau_{i_2} \cup \ldots \cup \tau_{i_k}$ belong to the same set. The subset of the form

$$p'_\sigma = p_{\bigcup_{i\in\sigma} \tau_i}$$

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 $S = C_1 \cup C_2 \cup \ldots \cup C_l$ 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 α a real number then for $\varepsilon > 0$ the inequality $|e^{2\pi i p_\sigma \alpha} - 1| < \varepsilon$ has a solution for some $\sigma \in \mathscr{F}$.*

Proof. Divide the unit circle into small arcs Δ_j, and set

$$p_\sigma \in C_j \Leftrightarrow e^{2\pi i p_\sigma \alpha} \in \Delta_j.$$

By Theorem 3, for some σ, τ, p_σ, p_τ and $p_{\sigma\cup\tau}$ belong to the same C_j. So

$$\zeta_\sigma = \exp(2\pi i p_\sigma \alpha), \quad \zeta_\tau = \exp(2\pi i p_\tau \alpha) \quad \text{and} \quad \zeta_\sigma \zeta_\tau$$

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

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

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

$$x'_\sigma = x_{\bigcup_{i\in\sigma} \tau_i}$$

then $\{x'_\sigma\}$ is an $\mathscr{F}$-subsequence of $\{x_\sigma\}$. Notice that an $\mathscr{F}$-subsequence of an IP-set in Z is again an IP-set. Also notice that an $\mathscr{F}$-subsequence of an $\mathscr{F}$-subsequence is an $\mathscr{F}$-subsequence.

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

$$IP\text{-}\lim_\sigma x_\sigma = x \in X \quad \text{or} \quad x_\sigma \to x$$

if, for any $\varepsilon > 0$, there exists $\sigma(\varepsilon)$ such that whenever $\sigma \cap \sigma(\varepsilon) = \emptyset$ (i.e., σ 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 $\mathscr{F}$-sequence in X has a convergent $\mathscr{F}$-subsequence.*

2. IP-recurrence.

DEFINITION. A function $f(n)$ on $\mathbf{Z}$ with values in a compact metric space is *IP-recurrent* ($f \in IPR$, or f *is IPR*) if for any IP-set $\{p_\sigma\}$ there exists an $\mathscr{F}$-subsequence $\{p'_\sigma\}$ so that

$$IP\text{-}\lim_\sigma f(n+p'_\sigma) = f(n) \tag{7}$$

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

The crucial property for us is the following:

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

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

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 $\mathbf{C}$. 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

$$IP\text{-}\lim_\sigma f(n+p_\sigma) = f(n)$$

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

$$g'(n) = IP\text{-}\lim_\sigma g(n+p_\sigma).$$

Then

$$g'(n+1)g'(n)^{-1} = IP\text{-}\lim_{\sigma} g(n+1+p_\sigma)g(n+p_\sigma)^{-1}$$
$$= IP\text{-}\lim_{\sigma} f(n+p_\sigma) = f(n)$$
$$= g(n+1)g(n)^{-1}.$$

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

$$IP\text{-}\lim_{\sigma} g(n+p_\sigma) = \gamma g(n).$$

For some σ_0, if $\sigma \cap \sigma_0 = \emptyset$, we will have

$$(8) \qquad |g(p_\sigma) - \gamma g(0)| < \varepsilon.$$

For τ with $\tau \cap \sigma_0 = \emptyset$ and $\tau \cap \sigma = \emptyset$ we will have

$$(9) \qquad |g(p_{\sigma\cup\tau}) - \gamma g(0)| < \varepsilon.$$

For some σ_1, if $\tau \cap \sigma_1 = \emptyset$, we will have, in addition,

$$(10) \qquad |g(p_\sigma + p_\tau) - \gamma g(p_\sigma)| < \varepsilon.$$

Since $\{p_\sigma\}$ is an IP-set, $p_{\sigma\cup\tau} = p_\sigma + p_\tau$. We then have

$$(11) \qquad |g(p_\sigma+p_\tau) - \gamma^2 g(0)| < 2\varepsilon, \quad |g(p_\sigma+p_\tau) - \gamma g(0)| < \varepsilon.$$

Since $\varepsilon > 0$ is arbitrary we deduce that $\gamma = 1$ and this proves the theorem. ∎

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 $\varphi\colon X \to Y$ 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 $\exp(2\pi i n\alpha)$ 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 λ, $\exp(2\pi i\lambda f(n))$ 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 α, $f(n) = n\cos n\alpha$ 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 $f \in LIPR$. Then the function $g(n)f(n)$ is in $LIPR$.*

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

$$(12) \qquad \exp\big(2\pi i\lambda g(n)f(n)\big) = \sum_j p_j\big(g(n)\big)\exp\big(2\pi i\lambda t_j f(n)\big).$$

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

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 ΔF the function $\Delta F(n) = F(n+1) - F(n)$. Then Theorem 7 tells us that $\Delta f \in LIPR$ implies that $f \in LIPR$. Now let us define a space of function as follows.

DEFINITION. $\mathcal{L}$ denotes the smallest space of functions on $\mathbf{Z}$ 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 $\mathcal{L}_\alpha$ 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. $\mathcal{L} \subset LIPR$.

Proof. We verify by Theorem 7 and Lemma 9 that $LIPR$ has properties (i), (ii), and (iii). ∎

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

(i) If $\Delta f \in \mathcal{L}_{\nu-1}$ then $f \in \mathcal{L}'_\nu$.

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

LEMMA 11. *Each of the spaces $\mathcal{L}_\nu$ is translation invariant and $\mathcal{L}_\nu\mathcal{L}_\mu \subset \mathcal{L}_{\nu+\mu}$.*

Proof. Both statements are proved by induction. Translation invariance passes from $\mathcal{L}_0$ to $\mathcal{L}'_1$ 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 $f \in \mathcal{L}'_\mu$, $g \in \mathcal{L}'_\nu$. Then

$$\Delta fg(n) = f(n+1)g(n+1) - f(n)g(n) = \Delta f(n)g(n+1) + f(n)\Delta g(n),$$

so

$$\Delta fg \in \mathcal{L}'_{\mu-1}\mathcal{L}'_\nu + \mathcal{L}'_\mu\mathcal{L}'_{\nu-1} \subset \mathcal{L}_{\mu+\nu-1} \quad \text{and} \quad fg \in \mathcal{L}'_{\mu+\nu} \subset \mathcal{L}_{\mu+\nu}.$$

To check the product of elements in $\mathscr{L}_\mu$ and $\mathscr{L}_\nu$ it suffices to consider $(h_1 f)(h_2 g)$ with $h_1, h_2 \in \mathscr{R}$, $f \in \mathscr{L}'_\mu$, $g \in \mathscr{L}'_\nu$ but this case follows immediately. ∎

THEOREM 12. *The space $\mathscr{L}$ is the union of $\mathscr{L}_\nu$ and forms an algebra.*

Proof. Since $\bigcup \mathscr{L}_\nu$ has the properties of the definition of $\mathscr{L}$ we must have $\mathscr{L} = \bigcup \mathscr{L}_\nu$. ∎

Clearly $\mathscr{L}$ contains all polynomials. An example of a non-polynomial function in $\mathscr{L}_1$ is

$$g(n) = [\alpha n + \tfrac{1}{2}]$$

where α is irrational. To see this note that

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

is a periodic function of x with discontinuities when

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

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

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

and since $l(n\alpha)$ is in $\mathscr{L}_0$, we have $g \in \mathscr{L}_1$.

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

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

LEMMA 13. *For all x, y*

$$h_\theta(x) - h_\theta(y) = h_\theta(x-y) + G_\theta(\exp 2\pi i x, \exp 2\pi i y) \tag{13}$$

where $G_\theta(z, w)$ is a bounded integer valued function on the torus continuous except along the curves $z = e^{2\pi i\theta}$, $w = e^{2\pi i\theta}$, $zw^{-1} = e^{2\pi i\theta}$.

Proof. Since $h_\theta(x+1) = h_\theta(x)$, G_θ defined by (13) is a function on the torus and it can be discontinuous only if either $h_\theta(x)$, $h_\theta(y)$ or $h_\theta(x-y)$ is discontinuous. Since $h_\theta(x) \equiv x \pmod 1$ it follows that G_θ is integer valued and it is bounded since h_θ is bounded. ∎

We now prove

PROPOSITION 14. *For each function $f \in \mathscr{L}$ there is a countable set $\Theta(f) \subset \mathbf{R}$ such that if $\theta \notin \Theta(f)$ then $h_\theta(f(n))$ is a function in $\mathscr{L}$.*

Proof. We prove this for $f \in \mathscr{L}_\nu$ by induction on ν. For $f \in \mathscr{L}_0$ $f(n)$ is finite valued and *IPR*. For all but countably many values of θ, h_θ is continuous on the range of $f(n)$. By Theorem 8, $h_\theta(f(n))$ is again *IPR*, and

so $h_\theta \circ f \in \mathscr{L}_0$. Assume the proposition valid for functions in $\mathscr{L}_{\nu-1}$. If $f \in \mathscr{L}'_\nu$ then $\Delta f \in \mathscr{L}_{\nu-1}$. Consider now $h_\theta \circ f$. We have by Lemma 13,

$$h_\theta \circ f(n+1) - h_\theta \circ f(n) = h_\theta(\Delta f(n)) + G_\theta(\exp 2\pi i f(n+1), \exp 2\pi i f(n)). \tag{14}$$

Hence if $\theta \notin \Theta(\Delta f) \cup \bigcup_n (f(n) + \mathbf{Z})$, the function to the right of (14) is in $\mathscr{L}$, since $\exp 2\pi i f(n)$ is in *IPR* and G_θ is continuous at the points under consideration.

Next suppose $f = \sum_1^J g_j f_j$ where $f_j \in \mathscr{L}'_\nu$ and $g_j \in \mathscr{R}$. Let the range of g_j be $\{t_{j1}, t_{j2}, \ldots, t_{jq_j}\}$. We find polynomials p_{jq}, $1 \leqslant q \leqslant q_j$ so that $p_{jq}(t_{jq'}) = \delta_{qq'}$. We now check that

$$h_\theta \circ f(n) = h_\theta\Big(\sum_1^J g_j(n) f_j(n)\Big)$$

$$= \sum_{r_1,\ldots,r_J} p_{1r_1}(g_1(n)) \ldots p_{Jr_J}(n)\, h_\theta\Big(\sum_{j=1}^J t_{jr_j} f_j(n)\Big).$$

Since $\sum_{j=1}^J t_{jr_j} f_j \in \mathscr{L}'_\nu$, the function $h_\theta\big(\sum_{j=1}^J t_{jr_j} f_j(n)\big)$ will be in $\mathscr{L}$ provided θ avoids the countable set $\Theta\big(\sum_{j=1}^J t_{jr_j} f_j\big)$. Moreover each $p_{jr_j}(g_j(n))$ is in $\mathscr{L}_0 = \mathscr{R}$. Hence we may take

$$\Theta(f) = \bigcup_{r_1,\ldots,r_J} \Theta\Big(\sum_{j=1}^J t_{jr_j} f_j\Big)$$

and for $\theta \notin \Theta(f)$, $h_\theta \circ f \in \mathscr{L}$. ∎

4. Applications to diophantine approximation. Let

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

PROPOSITION 14′. *Let $f_1(n), f_2(n), \ldots, f_r(n)$ be functions in $\mathscr{L}$. Then if $\theta \notin \Theta(f_r)$ and $p(x_1, x_2, \ldots, x_r)$ is any real polynomial, the function*

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

is in $\mathscr{L}$.

Proof. We can write $f(n) = p'\big(f_1(n), f_2(n), \ldots, f_{r-1}(n), f_r(n), h_\theta \circ f_r(n)\big)$ for some other polynomial p'. Since $\mathscr{L}$ is an algebra and each of the functions in question is in $\mathscr{L}$ so is f. ∎

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

$$|p(x_1, x_2, \ldots, x_l) - y| < \varepsilon \tag{15}$$

where $y, x_1, \ldots, x_l \in Z$. For ε small (15) is equivalent to

(i) $|e^{2\pi i p(x_1, x_2, \ldots, x_l)} - 1| < 2\sin \pi\varepsilon = \delta$,

(ii) $y =$ integer nearest $p(x_1, x_2, \ldots, x_l)$.

If $\varepsilon - 1 < \theta < -\varepsilon$, then (15) implies that the integer nearest $p(x_1, x_2, \ldots, x_l)$ is $I_\theta(p(x_1, x_2, \ldots, x_l))$. Thus (15) is equivalent to (i) and

(ii′) $y = I_\theta(p(x_1, x_2, \ldots, x_l))$ for $\varepsilon - 1 < \theta < -\varepsilon$.

THEOREM 15. *Let $p_1(t_1), p_2(t_1, t_2), \ldots, p_l(t_1, t_2, \ldots, t_l)$ be real polynomials vanishing for $t_1 = t_2 = \ldots = t_l = 0$. Then for any $\varepsilon > 0$ there exist integer solutions, not all 0, to*

$$(15)\qquad \begin{aligned} &|p_1(x_1) - x_2| < \varepsilon, \\ &|p_2(x_1, x_2) - x_3| < \varepsilon, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &|p_l(x_1, x_2, \ldots, x_l) - x_{l+1}| < \varepsilon. \end{aligned}$$

Proof. We form functions in $\mathscr{L}$ inductively setting

$$(16)\qquad \begin{aligned} &f_1(n) = p_1(n), \\ &f_2(n) = p_2(n, I_{\theta_1}(f_1(n))), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &f_l(n) = p_l(n, I_{\theta_1}(f_1(n)), \ldots, I_{\theta_{l-1}}(f_{l-1}(n))). \end{aligned}$$

The θ_i are chosen inductively in the interval $(\varepsilon - 1, -\varepsilon)$ and so that the function f_{i+1} remains in $\mathscr{L}$ in accordance with Proposition 14′. Thus the functions

$$\varphi_j(n) = e^{2\pi i f_j(n)}$$

are all *IPR* functions which for $n = 0$ take on the value 1.

Now apply the corollary to Theorem 6 to the *IPR* functions φ_j. We can find n so that all

$$|\varphi_j(n) - 1| < \delta = 2\sin \pi\varepsilon, \quad j = 1, 2, \ldots, l.$$

Thus the distance of each $f_j(n)$ to the nearest integer is $< \varepsilon$. Hence

$$(17)\qquad |f_j(n) - I_{\theta_j}(f_j(n))| < \varepsilon.$$

Set $x_1 = n$, $x_2 = I_{\theta_1}(f_1(n))$, $x_3 = I_{\theta_2}(f_2(n)), \ldots, x_{l+1} = I_{\theta_l}(f_l(n))$; then (16) and (17) give

$$|p_j(x_1, x_2, \ldots, x_j) - x_{j+1}| < \varepsilon. \ \blacksquare$$

5. Recurrence along relatively dense sets. A subset $S \subset Z$ is called *relatively dense* (also *syndetic*) if finitely many translates of S cover Z. Equivalently S is relatively dense if S has bounded gaps.

LEMMA 16. *If $S \subset Z$ is not relatively dense, there is an IP-set $\{p_\sigma\}$ in Z which does not meet S.*

Proof. For every n there are intervals $(a_n, a_n + n) \subset Z \backslash S$. Choose $p_1 \in Z \backslash S$. Choosing an interval of length $|p_1|$ outside of S we find $p_2 \notin S$ with $p_2 + p_1 \notin S$. Continue inductively so that after $p_1, p_2, \ldots, p_l$ have been found so that no partial sum is in S, find an interval outside of S of length $> 2(|p_1| + |p_2| + \ldots + |p_l|) + 1$. If p_{l+1} is the midpoint of this interval then all $p_{i_1} + p_{i_2} + \ldots + p_{i_k} + p_{l+1} \notin S$ for $i_1 < i_2 < \ldots < i_k < l+1$. This proves the lemma. $\blacksquare$

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

$$d(f(p_\sigma), f(0)) < \varepsilon$$

for some p_σ. Consider the set S of n for which $d(f(n), f(0)) < \varepsilon$. If this set were not relatively dense, use the lemma to find an *IP*-set in the complement of S. Since 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 $n\cos n\alpha$. 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 $f(n) = n\cos nt$ is not in LIPR, and* $\exp(2\pi i n\cos nt)$ *is not in IPR.*

This proves that *LIPR* is not closed under multiplication.

Let T^Z denote the space of sequences $\{x_n\}_{n\in Z}$ with the product topology. We denote by σ the shift on T^Z: $(\sigma x)_n = x_{n+1}$. We define the *positive orbit* of a point $x \in T^Z$ as the set $\{\sigma^n x\} \subset T^Z$ 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 $c(t) = \{e^{2\pi i n\cos nt}\}_{n\in Z}$ is all of T^Z.*

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

$$|e^{2\pi i n\cos nt} + 1| < \sqrt{2}$$

and

$$|e^{2\pi i n\cos nt}-1|>\sqrt{2}.$$

By Theorem 17, $e^{2\pi i n\cos nt}$ cannot be *IPR*.

We proceed to prove the proposition.

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

$$\{(e^{2\pi i n_k\cos n_k t}, e^{2\pi i(n_k+1)\cos(n_k+1)t}, \ldots, e^{2\pi i(n_k+d-1)\cos(n_k+d-1)t})\}$$

is equidistributed on the d-torus for a.e. t. In particular it will follow that the positive orbit closure is all of $T^{\mathbf{Z}}$. LeVeque ([8]) has shown that for a.e. t $e^{2\pi i n\cos nt}$ 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, $0\leqslant j<d$ not all zero and any fixed m we have*

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

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 $f_n'(t)-f_m'(t)$ has at most $O(n)$ zeros in $[0, 2\pi]$, and the same is true for $f_n''-f_m''$. On each interval of monotonicity of $f_n'-f_m'$ we look at a subinterval (a, b) where this derivative has a value at least $n^{3/2}$. The standard estimates show that our integral evaluated over such an interval (a, b) is $O(1/n^{3/2})$ 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

$$|f_n'(t)|=\sum_0^{d-1}(n+j)^2 a_j\sin(n+j)t=n^2\sum_1^{d-1}\Big(1+\frac{j}{n}\Big)^2 a_j\sin(n+j)t$$

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

$$\sum_0^{d-1}\Big(1+\frac{j}{n}\Big)^2 a_j\sin(n+j)t=O(1/n^{1/2}).$$

However we can write this latter expression as

$$I_m\Big(e^{int}\sum_0^{d-1}\Big(1+\frac{\delta}{n}\Big)^2 a_j e^{ijt}\Big)=I_m(e^{int}Q_n(t))$$

where $Q_n(t)$ converges uniformly to a non zero polynomial of degree at most $d-1$. From this it easily follows that meas $\{t\colon |f_n'(t)-f_m'(t)|\leqslant n^{3/2}\}\to 0$ 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 $k_0\leqslant k<l$ one has

$$\int_0^{2\pi}\exp i\Big(\sum_0^{d-1}(n_k+j)a_j\cos(n_k+j)t-\sum_0^{d-1}(n_l+j)a_j\cos(n_l+j)t\Big)dt<2^{-k}.$$

It follows that

$$\int_0^{2\pi}\Big|\frac{1}{N}\sum_{k=1}^{N}\exp i\Big(\sum_0^{d-1}(n_k+j)a_j\cos(n_k+j)t\Big)\Big|^2 dt=O(1/N)$$

and thus

$$\sum_{N=1}^{\infty}\int_0^{2\pi}\Big|\frac{1}{N^2}\sum_{k=1}^{N^2}\exp i\Big(\sum_0^{d-1}(n_k+j)a_j\cos(n_k+j)t\Big)\Big|^2 dt<\infty.$$

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

$$g_{N^2}=\frac{1}{N^2}\sum_{k=1}^{N^2}\exp i\Big(\sum_0^{d-1}(n_k+j)a_j\cos(n_k+j)t\Big)\to 0$$

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

[1] L. Auslander, L. Green, and F. Hahn, *Flows on Homogeneous Spaces*, Annals of Math. Study #53, Princeton 1963.

[2] W. Furstenberg, *Recurrence in Ergodic Theory and Combinatorial Number Theory*, Princeton 1981.

[3] — *IP-systems in ergodic theory*, Contemporary Mathematics 26 (1982), pp. 131–138.

[4] H. Furstenberg and B. Weiss, *Combinatorial number theory and topological dynamics*, Journal d'Anal. Math. 34 (1978), pp. 61–85.

[5] R. Graham, B. Rothschild, and J. Spencer, *Ramsey Theory*, New York 1980.

[6] N. Hindman, *Finite sums from sequences within cells of a partition of IN*, J. Comb. Theory (A) 17 (1974), pp. 1–11.

[7] J. Koksma, *Diophantische Approximationen*, Berlin 1936.

[8] W. LeVeque, *The distribution* mod 1 *of trigonometric sequences*, Duke Math. J. 20 (1953), pp. 367–374.

[9] H. Weyl, *Über die Gleichverteilung die Zahlen* mod *Eins*, Math. Annalen 77 (1916), pp. 313–352.

INSTITUTE OF MATHEMATICS
HEBREW UNIVERSITY
Jerusalem, Israel

Received on 27.6.1986 (1659)

ACTA ARITHMETICA
XLIX (1988)

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*

$$\sigma^2 = \sum_{n=1}^{\infty} r_n^2 < \infty, \tag{1}$$

and put $X = \sum_{n=1}^{\infty} r_n X_n$. If N and V are chosen so that $\sum_{n \le N} r_n \le V/2$, then

$$P(X \ge V) \le \exp\Big(-\tfrac{1}{8} V^2 \Big(\sum_{n>N} r_n^2\Big)^{-1}\Big). \tag{2}$$

If $\sum_{n \le N} r_n \ge 2V$ then

$$P(X \ge V) \ge 2^{-22} \exp\Big(-120 V^2 \Big(\sum_{n>N} r_n^2\Big)^{-1}\Big). \tag{3}$$

Also, if $\sum_{n \le N} r_n \ge V$ then

$$P(X \ge V) \ge 2^{-N-1}. \tag{4}$$

---

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