WILLIAM A. VEECH

Ergodic theory and uniform distribution

Astérisque, tome 61 (1979), p. 223-234

<http://www.numdam.org/item?id=AST_1979__61__223_0>
Ergodic Theory and Uniform Distribution
by
William A. Veech*

1. Introduction. We shall discuss the applications of ergodic theory to two problems in the theory of uniform distribution. The first problem concerns uniform distribution in a general compact group, the second uniform distribution modulo 1.

If $K$ is a compact (Hausdorff, topological) group, a sequence $S = \{s_n\}$ in $K$ is a $K$-sequence if $S$ generates a dense subgroup of $K$. $S$ is a $K_\sigma$-sequence if it has the additional properties that (i) for every $n > 0$ $(s_1, \ldots, s_n) = (s_{k+1}, \ldots, s_{k+n})$ for infinitely many $k$, and (ii) $S^{-1}S = \{s_{-1}^1, s_{-1}^2\}$ generates a dense subgroup of $K$. Any $K$-sequence may be used to construct a $K_\sigma$-sequence.

We recall that a sequence $R = \{r_n\}$ is called a uniformly (resp. well) distributed sequence generator, u.d.s.g. (resp. w.d.s.g.), if for every compact group $K$ and every $K$-sequence $S \subset K$, the sequence $T(R, S) = \{t_n\}$, where

\begin{equation}
(1.1) \quad t_n = \prod_{j=1}^{n} s_j r_j
\end{equation}

is uniformly (resp. well) distributed in $K$ ([13], [15], [17]).

Examples of u.d.s.g.'s are given in [13], [15]. One such is $r_1 = 9$, $r_2 = 2$, and in general $r_n$ is the length of the gap between the $n^{th}$ and $(n+1)^{st}$ '1' in the sequence 123456789101112... .

At the present time one knows no example of a w.d.s.g. . However, Losert and Rindler [8] have proved there exist sequences $R \subset \mathbb{Z}$ which satisfy a similar condition which we shall not describe.

*Research supported by NSF - MCS 78-01858
Any Losert-Rindler sequence serves as a "program" (like (1.1)) for writing down a well distributed sequence in terms of a given K-sequence. This is the purpose for which the notion of a w.d.s.g. was introduced, and the Losert-Rindler result suffers only an aesthetic defect of being nonexplicit.

In preparation of the statement of the first theorem, let
\[ \lambda = \{\lambda_1, \lambda_2, \ldots\} \]
be a sequence of integers such that \( \lambda_n \geq 2 \). Also, set \( \lambda_0 = 1 \). For every \( k \in \mathbb{Z} \) such that \( k \neq -1 \) there is a unique integer \( \tau = \tau(k) \geq 0 \) such that
\[
(1.2) \quad k+1 = \lambda_0 \lambda_1 \cdots \lambda_\tau (a_\tau + b)
\]
with \( a \in \mathbb{Z} \) and \( 0 < b < \lambda_{\tau+1} \).

Notice in the theorem to follow that the \( K_\sigma \)-sequence begins at 0 (the definition is analogous).

1.3 Theorem. With notations as above, assume the sequence \( \lambda \) is bounded, and define \( R = \{\tau(1), \tau(2), \ldots\} \). If \( K \) is a compact group, and if \( S = \{s_0, s_1, \ldots\} \) is a \( K_\sigma \)-sequence in \( K \), then \( T(R, S) \) (see (1.1)) is well distributed in \( K \).

Next, let \( X = \mathbb{R}/\mathbb{Z} \), and let \( \alpha \in X \) be an irrational. Given an "interval" \( I \subset X \) whose length is denoted \( |I| \), define \( S_n(x) = S_n(x, \theta, I) \), \( x \in X \), \( n > 0 \), to be the number of \( j \) such that \( 0 \leq j < n \) and \( x+j\alpha \in I \).

A theorem of Kesten [7] asserts that there exists \( x \in X \) such that \( S_n(x) - n|I| \) is bounded (in \( n \)) only if \( |I| \in \mathbb{Z}\alpha \) modulo 1. (The converse is easy and classical.) A simple proof of Kesten's theorem is given by Furstenberg-Keynes-Shapiro [6] (see also [17]). The following is a sharpening of Kesten's theorem:
1.4 Theorem. *With notations as above, suppose there exist* $x \in X$ and $M < \infty$ *such that*

$$E_M(x) = \{n \mid |S_n(x) - n| \leq M\}$$

*has positive upper density.* Then modulo 1, $|I| \in \mathbb{Z}^\mathbb{R}$.

2. Monothetic groups. In this section $X$ denotes an infinite compact monothetic group and $\theta \in X$ an element which generates a dense subgroup. $X$ will be written additively. Let $\mu$ be normalized Haar measure on $X$.

Fix a finite set $E \subseteq X$ such that $E$ contains a coset of no subgroup of $X$ other than $\{0\}$. Let $K$ be a compact group, and let there be given a continuous map $\varphi : E^c \to K$ such that $\varphi$ does not extend to be continuous on $X$.

Define $X' = E + \mathbb{Z}\theta$, and define a map $X' \to K^\mathbb{Z}$ by $m_x(n) = \varphi(x + n\theta)$, $x \in X'$, $n \in \mathbb{Z}$. The closure, $M$, of the image of $X'$ is invariant under the left shift, $\sigma(m(n) = m(n+1))$. In addition one has from [16], Section 2, that (a) $(\sigma, M)$ is minimal (every $\sigma$-orbit in $M$ is dense in $M$), (b) $(\sigma, M)$ is uniquely ergodic (there is a unique normalized $\sigma$-invariant Borel measure on $M$), and (c) the map $\pi_m = x$, $x \in X'$, is well defined and extends to a continuous map $M \to X$ such that $\pi_m = \pi_m + \theta$, $m \in M$; moreover, $\pi$ is one-to-one on $\pi^{-1}X'$. Because of (b) and (c), we shall write $\mu$ also for the normalized invariant measure on $M$.

Next, let $N = M \times K$, and define $T : N \to N$ by

$$(2.1) \quad T(m,k) = (\sigma m, m(0)k)$$

Let $\nu$ be normalized Haar measure on $K$, and set $\omega = \mu \times \nu$. Clearly, $\omega$ is $T$-invariant.
If \((T,N)\) is uniquely ergodic, a theorem of Oxtoby [9] implies that for each \(z \in N\) the sequence \(\{T^nz, n \geq 1\}\) is \(\omega\)-well distributed in \(N\). In particular, the sequence of "second coordinates" is well distributed in \(K\). When \(z = (m_x,e), x \in X',\) the second coordinate of \(T^nz, n > 0,\) is

\[
\varphi^{(n)}(x) = \varphi(x+(n-1)e)\varphi(x+(n-2)e)\ldots\varphi(x).
\]

It is Furstenberg's observation that \((T,N)\) is uniquely ergodic if \(\omega\) is ergodic for \(T\) (if \(A \subset N\) is measurable, and if \(T^{-1}A = A\), then \(\omega(A) = 0\) or \(\omega(A^c) = 0\)([5])). The necessary and sufficient condition that \(\omega\) fail to be ergodic is that there exist a nontrivial continuous irreducible unitary representation \(\rho:K \to U(d)\) and a nonconstant measurable function \(F:X \to \mathbb{C}^d\) such that

\[
F(x+\theta) = \rho(\varphi(x))F(x) \quad (a.e. \mu).
\]

(See [5], [14].)

3. Proof of Theorem 1.3. Let \(\lambda\) be as in the introduction, and define \(\lambda_0 = 0\) and \(\lambda_n = \lambda_1\lambda_2\ldots\lambda_n, n > 0.\) We set \(X = \lim_{n \to \infty} \mathbb{Z}/\lambda_n\mathbb{Z}\) and view \(X\) as the set of sequences, \(x = (x_1,x_2,...),\) such that \(0 \leq x_n = x_n(x) < \lambda_n\) and \(x_{n+1} - x_n \in \lambda_n\mathbb{Z}\) for all \(n > 0.\) Letting \(\theta = (1,1,...),\) the subgroup \(\mathbb{Z}\theta\) is dense in \(X.\) \(\mu\) denotes normalized Haar measure on \(X.\)

Let \(E = \{-\theta\}.\) If \(x \not\in E,\) define \(\tau(x) = t-1,\) where \(t\) is the least integer such that \(x_\downarrow \not\in \lambda_{t-1}.\) \(\tau(\cdot)\) is continuous on \(E^c,\) and

\[
\lim_{x \to \theta} \tau(x) = \infty.\]

In terms of the function \(\tau(k), k \not\in t-1,\) defined in (1.2), one has (a) \(\tau(k\theta) = \tau(k), k \not\in -1,\) and (b) \(\tau(x) = \tau(x_n(x))\) for any \(n\) such that \(x_n(x) \not\in \lambda_n-1.\)
Define partitions $\mathcal{P}_n = \{P_{nk} \mid 0 \leq k < n\}$ by setting $P_{nk} = \{x \mid x \in (x) = k\}$. The function $T_n(x) = \wedge_n -1 - x_n(x)$ assumes the constant value $\wedge_n -1 - k$ on $P_{nk}$ for each $k$. Remark (b) of the preceding paragraph implies $\tau(x+q)$ is constant on $P_{nk}$ if $q \neq \wedge_n -1 - k$. As for the exceptional value of $j$, define $P_{nk}^t = \{x \in P_{nk} \mid \tau(x+(\wedge_n -1 - k)\theta) = n+\ell\}$, $\ell \geq 0$. An easy counting argument shows $\mu(P_{nk}^t) = (\wedge_n + \ell - 1) \wedge_n - 1 \mu(P_{nk})$ holds for $\ell \geq 0$. If in particular $\lambda$ is bounded (by $Q$), the last inequality implies

$$\mu(P_{nk}^t) \geq Q^{-(\ell+1)} \mu(P_{nk}) .$$

If $x \in X$, write $P_n = P_n(x)$ for the element of $\mathcal{P}$ which contains $x$. Given an $L^1(\mu)$ function $F:X \to \mathbb{C}^d$, the martingale theorem, together with a standard argument, shows

$$\lim_{n \to \infty} \frac{1}{\mu(P_n)} \int \{F(y) - F(x)\} |\mu(dy) = 0 .$$

Next, suppose $K \neq \{e\}$ is a compact group, and let $S = \{\psi(0), \psi(1), \ldots\}$ be a $K \sigma$-sequence in $K$. Using $\tau$ and $S$, we define $\psi(x) = \psi(\tau(x))$, $x \in E^C$. The facts $K \neq \{e\}$ and $S$ is a $K \sigma$-sequence easily imply $\psi$ has no limit at $-\theta$. We shall be interested in $\psi(\wedge_n)$ which we denote by $\psi_n$. Our earlier discussion implies there exist $A_{nk}, B_{nk} \in K$, $0 \leq k \leq \wedge_n$, such that

$$\psi_n(x) = A_{nk} \psi(n+\ell) B_{nk} \quad (x \in P_{nk}^t) .$$

Indeed, of the $\wedge_n$ factors determining $\psi_n$, all but one are constant on $P_{nk}$, and that factor is constantly $\psi(n+\ell) = \psi(\tau(x+T_n(x)\theta))$ on $P_{nk}^t$.

Suppose now that $\rho$ is a nontrivial continuous irreducible unitary representation of $K$ on $\mathbb{C}^d$, and suppose also that (2.3) has a nontrivial measurable solution. We replace $K$ by $\rho(K) \neq \{e\}$, and reletter, so that (2.3) becomes
(2.3') \quad F(x+\theta) = \phi(x)F(x) .

Now \( \phi(x) \in U(d) \), and (2.3') implies \(|F(\cdot)|\) is invariant under translation by \( \theta \), hence constant a.e. As \( F \) is assumed to be nontrivial, we may and shall assume that \(|F(x)| = 1 \) a.e. This will lead us to a contradiction, assuming \( \lambda \) is bounded (by \( Q \)).

Iterating (2.3'), one finds \( F(x+m\theta) = \phi^m(x)F(x) \), and this, plus the continuity of translation in \( L^1(u) \), implies

\[
(3.4) \quad \lim_{m \to 0} \|\phi^m(F) - F\|_1 = 0 .
\]

3.5 Lemma. With notations as above, there exists for every pair \( \epsilon, q > 0 \) a vector \( v = v(\epsilon, q) \), \(|v| = 1 \), such that \(|\psi(i)v - \psi(j)v| < 2\epsilon\), \( 0 \leq i, j \leq q \).

Proof: \( S \) is a \( K_\sigma \)-sequence, and therefore there exists an infinite set \( \tau \) such that \( \psi(n+j) = \psi(j) \), \( 0 \leq j \leq q \), \( n \in \tau \). Apply (3.4) \( (m = \Lambda_n, n \in \tau) \), and (3.2) to conclude that if \( n \in \tau \) is large there exist \( p_{nk} \in \Phi_n \), such that \( (p_{nk}^\epsilon)^c = \{ y \in \Phi_n \mid |\psi(y)F(x) - F(x)| \geq \epsilon \} \) has measure less than \( Q^{-(q+1)}(\epsilon)\). From (3.1) one concludes \( p_{nk}^\epsilon \cap p_{nk}^\epsilon \neq \emptyset \), \( 0 \leq t \leq q \). Finally, (3.3), the definition of \( p_{nk}^\epsilon \), and the facts \( n \in \tau \) and \( A_{nk} \in U(d) \) imply that if \( v = p_{nk}^\epsilon F(x) \), then \(|v| = 1 \) and

\[
|\psi(i)v - \psi(j)v| < 2\epsilon, \quad 0 \leq i, j \leq q .
\]

The lemma is proved.

Notice in the above that also \(|\psi(i)^{-1}\psi(j)v - v| < 2\epsilon\), \( 0 \leq i, j \leq q \), \( v = v(\epsilon, q) \). If we let \( \epsilon \to 0 \), \( q \to \infty \) in such a way that \( v(\epsilon, q) \to v_0 \), then \(|v_0| = 1 \), and \( \psi(i)^{-1}\psi(j)v_0 = v_0 \), \( i, j \geq 0 \). As \( S \) is a \( K_\sigma \)-sequence \( kv_0 = v_0 \), \( k \in K \). Irreducibility then implies \( d = 1 \), \( K = \{ e \} \), a contradiction. We conclude that (2.3) cannot have a nontrivial measurable solution. The discussion of Section 2 now implies Theorem 1.3. (The second coordinate of \( T^n(\theta, \epsilon) \) is \( \phi^{(n)}(\theta) = \psi(\tau(n))\psi(\tau(n-1))...\psi(\tau(1)) \), where \( \tau(k) \) is defined by (1.2)).
Remark on the case \( d = 1 \). Let \( \lambda \) be as in Section 1, possibly unbounded, and let \( S = \{ \psi(n) \}_{n \geq 0} \) be a sequence of complex numbers of absolute value 1. Define \( K \) to be the closed subgroup of \( U(1) \) generated by the terms of \( S \). Form \( X = X(\lambda) \), and set \( \phi(x) = \psi(\tau(x)), \ x \neq \theta \). We wish to allow for the possibility that \( \omega \) has a limit at \( -\theta \); this means that \( M = M(\lambda, \psi) \), rather than having \( X(\lambda) \) for a "factor," may in fact itself be a "factor" of \( X(\lambda) \) (more precisely, the quotient of \( X(\lambda) \) by the periods of the extended function \( \omega \)). Let \( N = N(\lambda, \psi) = M \times K \) and \( T = T(\lambda, \psi) \) be as in Section 2. Also, set \( \omega = \omega(\lambda, \psi) = \cup \times \nu \), as in Section 2. Using the above, one may prove

3.6 Theorem. With notations as above, suppose \( \sum_{n=0}^{\infty} |\psi(n+1) - \psi(n)| = \infty \). Then \( (T, N) \) is uniquely ergodic. Moreover, the point spectrum of \( T \), relative to \( \omega \), is contained in \( \Gamma(\lambda) = \{ \chi(\theta) | x \text{ a continuous character on } X(\lambda) \} \).

If \( \tilde{\lambda} \) is a second sequence, we write \( \tilde{\lambda} \perp \lambda \) if \( \langle \lambda_n, \tilde{\lambda}_n \rangle = 1 \) for all \( n \). When \( \tilde{\lambda} \perp \lambda \), the Chinese Remainder Theorem implies \( Z(\theta, \tilde{\theta}) \) is dense in \( X(\lambda) \times X(\tilde{\lambda}) \), and this in turn implies \( \sigma \times \tilde{\sigma} \) is uniquely ergodic on \( M \times \tilde{M} \) for any given \( \tilde{\psi} \). Suppose now that both \( \psi \) and \( \tilde{\psi} \) satisfy the hypothesis of Theorem 3.6. As \( \Gamma(\lambda) \cap \Gamma(\tilde{\lambda}) = \{ 1 \} \), the point spectra of \( T, \tilde{T} \), relative to \( \omega, \tilde{\omega} \), have trivial intersection (\( \{ 1 \} \)), and so by a well known result in ergodic theory, \( T \times \tilde{T} \) is ergodic relative to \( \omega \times \tilde{\omega} \). But \( \omega \times \tilde{\omega} \) may be viewed as \( (\cup x_U) \times (\cup x_{\tilde{\nu}}) \), \( \cup x_{\tilde{\nu}} = \text{Haar measure on } K \times \tilde{K} \), and so Furstenberg's principle (Section 2), plus the unique ergodicity of \( \sigma \times \tilde{\sigma} \), implies \( T \times \tilde{T} \) is uniquely ergodic.

The sequences \( \varphi^{(n)}(0), \tilde{\varphi}^{(n)}(0) \) are "q-multiplicative sequences"
(see [3] for definition and references). An immediate consequence
of the above is that when \( \lambda \perp \lambda \) and \( \nu, \tilde{\nu} \) satisfy the hypothesis of
Theorem 3.6, one has

\[
\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} \phi(n) \tilde{\nu}(n) = 0.
\]

It would be interesting to know whether other known (and unknown)
properties of \( q \)-multiplicative sequences can be obtained from such
considerations.

4. Irregularities of distribution modulo 1. In this section we
suppose \( X = \mathbb{R}/\mathbb{Z} \), and we fix \( \theta \in X \) irrational. If \( I \subset X \) is an in-
terval and \( \alpha, \beta \in \mathbb{R} \), define \( \phi = (\alpha - \beta) x_I - \beta x_I \). We regard \( \phi \) as having
values in \( K = K(\alpha, \beta) \), the closed subgroup of \( X \) generated by \( \alpha \) and \( \beta \)
(modulo 1). We note that \( \phi(n)(x) = S_n(x)\alpha - n\beta \), where \( S_n(x) = S_n(x, \theta, I) \) is defined in Section 1.

Let \( \{p_n/q_n\} \) be the sequence of convergents to \( \alpha \), and define \( \Gamma_0(\alpha) \)
\( \in X \) to be the set of \( t \) which admit a representation \( t = \sum_{n=1}^{\infty} b_n q_n \beta \)
(in \( X \)) such that \( b_n \in \mathbb{Z} \) and \( \lim_n b_n q_n \|q_n \beta\| = 0 \). (Any two such repre-
sentations agree for large \( n \) [16].) If \( \alpha \in \mathbb{R} \), we also define \( \Gamma_0(\theta) = \{t \in \Gamma_0(\theta) | \lim_n b_n \alpha = 0 \text{ in } X \} \). As noted in [16], [17] we have (i)
if \( \alpha \) has bounded partial quotients, then \( \Gamma_0(\theta) = \mathbb{Z} \alpha \), and (i) if
\( t \not\in \mathbb{Z} \theta \), then for almost all \( \alpha \), \( t \not\in \Gamma_0(\theta) \).

The theorem below is proved in [16] for \( \alpha = \frac{1}{2} \). Extension to the
general case is sketched in [18], [17] and the details are carried
out by Stewart in [12].

4.1 Theorem. Let \( \alpha, \beta \in \mathbb{R} \), \( \alpha \not\in \mathbb{Z} \). If for every \( k \) such that
\( k\alpha \not\in 0 \text{ (in } X) \) \( |I| \not\in \Gamma_x(\theta) \) modulo 1, then \( (T, N) \) (Section 2) is uni-
que ergodic.
4.2 Corollary. ([17],[12]) If \(|l| \not\equiv 0 \mod 1\), then for almost all \(a \in \mathbb{R}\) the sequence \(\{S_n(x)a-n\beta\}\) is well distributed modulo 1 for any choice of \(x \in X\) and \(\beta \in \mathbb{R}\).

The corollary may be used to prove Theorem 1.4. To this end, suppose \(|l| \not\equiv 0 \mod 1\) but for some \(x \in X\) and \(M < \infty\) the set \(E^*_M(x)\) (Section 1) has upper density \(2\epsilon > 0\). Corollary 4.2 implies there exists \(\alpha, 0 < \alpha < \frac{\epsilon}{2M}\) such that \(\{S_n(x)a-n\beta\}\) is well distributed modulo 1 for all \(\beta\). Set \(\beta = |l|\alpha\), and note for this choice that \(\|S_n(x)a-n|l|\alpha\| < \frac{\epsilon}{2}\) if \(n \in E_N(x)\). Well distribution implies the set of \(n\) such that \(\|S_n(x)a-n|l|\alpha\| < \frac{\epsilon}{2}\) has upper density \(\frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon < 2\epsilon\), and we have a contradiction. That is, \(E_M(x)\) has upper density 0, and the theorem is proved.

When \(\omega = (\alpha-\beta)\chi_I-\chi_{I^c}\) is regarded as taking values in \(\mathbb{R}\), it is natural to prevent "drift" by requiring \(\omega\) to have integral 0. But for a change of scale, this is tantamount to requiring \(\omega = (1-|l|)\chi_I-|l|\chi_{I^c}\). In what follows, \(G = G(I)\) is the closed subgroup of \(\mathbb{R}\) generated by \(|l|\) and \(1-|l|\). We assume \(0 < |l| < 1\).

Define \(T:X \times G \rightarrow X \times G\) by \(T(x,y) = (x+\theta, y+\varphi(x))\). \(T\) preserves Haar measure on \(X \times G\), which of course is infinite. Using a topological analogue of K. Schmidt's notion of an "essential value" of a cocycle ([11]), it is not difficult to prove

4.3 Proposition. Assume \(|l|\) is rational or else 1, \(\theta\), and \(|l|\) are rationally independent. Then \(T\) has a residual set of points with dense orbits. In particular, for a residual set of \(x \in X\) the sequence \(S_n(x)-n|l|\) is dense in \(G(I)\).

One conjectures the conclusion of the proposition holds with
residual set of x replaced by 'measure 1 set of x.' (It does not hold for 'all x'. See Dupain [4].) One way to prove this is to prove T is ergodic (relative to Haar measure). This is so for |I| = \frac{1}{2} (K. Schmidt [10]; Conze-Keane [2]) and also for almost all values of |I| (Conze [1]). In [17] the question was raised whether |I| \not\in \Gamma_0(\Theta) implies ergodicity. This is proved by M. Stewart [12] when \Theta has bounded partial quotients, and Stewart now claims a proof for general \Theta (oral communication). It is open whether any condition on |I| is necessary for ergodicity (save |I| \in \Phi or 1, \alpha, |I| rationally independent).

Stewart's work relies heavily on the work of Schmidt and Conze. The most important ingredients are Schmidt's notion of essential value, the Denjoy-Koksma lemma (used by Conze), and the following

4.4 Theorem (M. Stewart [12]). Assume \Theta has bounded partial quotients. If t \not\in \mathbb{Z}^\alpha modulo 1, then

$$\limsup_{n \to \infty} (\|q_n t\| - \frac{1}{2} q_n \|q_n \Theta\|) > 0.$$ 

It would be of interest to have a formulation and proof of a nonabelian analogue of Theorem 4.1. At the present time one knows only that if \Theta has bounded partial quotients, if |I| \not\in \mathbb{Z}^\Theta modulo 1, and if K is a finite group with generators a, \Theta, the homeomorphism (T,N) corresponding to \varphi(x) = a, \Theta as x \in I, I^c is uniquely ergodic [14].

References


William A. VEECH
Department of Mathematics
Rice University HOUSTON
U.S.A.