UNIFORM DISTRIBUTION OF SEQUENCES IN RINGS OF INTEGRAL MATRICES

by HARALD NIEDERREITER and JAU-SHYONG SHIUE

(Received 1 May, 1978)

Dedicated to Professor L. Kuipers on the occasion of his 70th birthday

1. Introduction. For various discrete commutative rings a concept of uniform distribution has already been introduced and studied, for example, for the ring of rational integers by Niven [**9**] (see also Kuipers and Niederreiter [**2**, Ch. 5]), for the rings of Gaussian and Eisenstein integers by Kuipers, Niederreiter, and Shiue [**3**], for rings of algebraic integers by Lo and Niederreiter [**4**], [**7**], and for finite fields by Gotusso [**1**] and Niederreiter and Shiue [**8**]. In the present paper, we shall show that a satisfactory theory of uniform distribution can also be developed in a noncommutative setting, namely for matrix rings over the rational integers.

In general, given a sequence of elements of a discrete ring, one considers the way in which they are distributed among the residue classes modulo a left ideal of finite index. If each residue class contains asymptotically the same share of terms, the sequence is called uniformly distributed modulo the left ideal. In case this property is satisfied for all left ideals of finite index, the sequence is said to be (left) uniformly distributed in the ring. Analogous notions can, of course, be based on right ideals. In order to obtain the explicit character formulas needed for effective versions of the so-called Weyl criterion, one has to work with a concrete ring. Matrix rings over the rational integers have been chosen since they form standard examples of noncommutative rings but still allow a fairly rich theory.

2. Definitions and preliminaries. For a ring R and a positive integer m, let $\mathrm{Mat}_m(R)$ denote the full matrix ring of $m \times m$ matrices over R. We collect some information about the matrix ring $\mathrm{Mat}_m(\mathbf{Z})$, where $\mathbf{Z}$ is the ring of rational integers. Proofs of the following two results can be found in Newman [**5**, Ch. II].

LEMMA 2.1. *For any A in $\mathrm{Mat}_m(\mathbf{Z})$, there exist two unimodular matrices U and V such that UAV is a diagonal matrix.*

LEMMA 2.2. *Every left ideal of $\mathrm{Mat}_m(\mathbf{Z})$ is principal.*

If a matrix $A \in \mathrm{Mat}_m(\mathbf{Z})$ is given in terms of its entries a_{ij}, $1 \le i, j \le m$, we write $A = (a_{ij})$. The diagonal matrix with entries $b_1, \ldots, b_m$ on the main diagonal is denoted by $\mathrm{diag}(b_1, \ldots, b_m)$. For a nonsingular $G \in \mathrm{Mat}_m(\mathbf{Z})$, the following description of a complete residue system modulo G (i.e., modulo the principal left ideal generated by G) was given by Shiue and Hwang [**10**].

LEMMA 2.3. *Let $G \in \mathrm{Mat}_m(\mathbf{Z})$ be nonsingular, and let U and V be unimodular matrices such that UGV is a diagonal matrix, say $UGV = \mathrm{diag}(g_1, \ldots, g_m)$. Then $\{(r_{ij})V^{-1} : r_{ij} \in \mathbf{Z}, 0 \le r_{ij} < |g_j| \text{ for } 1 \le i, j \le m\}$ forms a complete residue system of $\mathrm{Mat}_m(\mathbf{Z})$ modulo G.*

https://doi.org/10.1017/S001708950000389X Published online by Cambridge University Press

COROLLARY 2.4. *For a nonsingular* $G \in \mathrm{Mat}_m(\mathbf{Z})$, *the cardinality of a complete residue system of* $\mathrm{Mat}_m(\mathbf{Z})$ *modulo* G *is* $|\det G|^m$.

Thus, the principal left ideal generated by a nonsingular $G \in \mathrm{Mat}_m(\mathbf{Z})$ is of finite index in $\mathrm{Mat}_m(\mathbf{Z})$. On the other hand, it is easily seen that the principal left ideal generated by a singular $G \in \mathrm{Mat}_m(\mathbf{Z})$ is not of finite index in $\mathrm{Mat}_m(\mathbf{Z})$.

Let $\{X_n\}$, $n = 1, 2, \ldots$, be a sequence of elements of $\mathrm{Mat}_m(\mathbf{Z})$. Then for a positive integer N and $B, G \in \mathrm{Mat}_m(\mathbf{Z})$ we use $A(N, B, G, \{X_n\})$ to denote the number of n, $1 \leq n \leq N$, such that $X_n \equiv B \bmod G$, i.e., such that $X_n - B$ lies in the principal left ideal generated by G.

DEFINITION 2.5. Let $G \in \mathrm{Mat}_m(\mathbf{Z})$ be nonsingular. Then the sequence $\{X_n\}$, $n = 1, 2, \ldots$, of elements of $\mathrm{Mat}_m(\mathbf{Z})$ is called *uniformly distributed modulo* G (abbreviated u.d. mod G) if

$$\lim_{N \to \infty} \frac{A(N, B, G, \{X_n\})}{N} = |\det G|^{-m} \tag{1}$$

holds for every $B \in \mathrm{Mat}_m(\mathbf{Z})$.

It is clear that it suffices to require (1) for every B from a complete residue system of $\mathrm{Mat}_m(\mathbf{Z})$ modulo G.

DEFINITION 2.6. The sequence $\{X_n\}$, $n = 1, 2, \ldots$, of elements of $\mathrm{Mat}_m(\mathbf{Z})$ is called *uniformly distributed in* $\mathrm{Mat}_m(\mathbf{Z})$ (abbreviated u.d. in $\mathrm{Mat}_m(\mathbf{Z})$) if it is u.d. mod G for all nonsingular $G \in \mathrm{Mat}_m(\mathbf{Z})$.

LEMMA 2.7. *If the sequence* $\{X_n\}$ *of elements of* $\mathrm{Mat}_m(\mathbf{Z})$ *is u.d.* mod G, *then the following holds.*

(i) $\{X_n + X\}$ *is u.d.* mod G *whatever the choice of* $X \in \mathrm{Mat}_m(\mathbf{Z})$.

(ii) $\{X_{n+h}\}$ *is u.d.* mod G *for every nonnegative integer* h.

(iii) $\{X_n V\}$ *is u.d.* mod UGV *for any unimodular* $U, V \in \mathrm{Mat}_m(\mathbf{Z})$.

Proof. All three properties follow easily from the definition.

An equivalent characterization of a u.d. sequence mod G is the following one.

THEOREM 2.8. *The sequence* $\{X_n\}$ *of elements of* $\mathrm{Mat}_m(\mathbf{Z})$ *is u.d.* mod G *if and only if for any two matrices* $B, C \in \mathrm{Mat}_m(\mathbf{Z})$ *we have*

$$\lim_{N \to \infty} \frac{A(N, B, G, \{X_n\})}{A(N, C, G, \{X_n\})} = 1. \tag{2}$$

Proof. The necessity is obvious. For the proof of the sufficiency, we fix $C \in \mathrm{Mat}_m(\mathbf{Z})$ and write (2) in the form

$$A(N, B, G, \{X_n\}) = A(N, C, G, \{X_n\}) + \mathrm{o}(A(N, C, G, \{X_n\})).$$

https://doi.org/10.1017/S001708950000389X Published online by Cambridge University Press

If $\mathfrak{J}$ is a complete residue system of $\mathrm{Mat}_m(\mathbf{Z})$ modulo G, we get

$$N=\sum_{B\in\mathfrak{J}} A(N,B,G,\{X_n\})=|\det G|^m A(N,C,G,\{X_n\})+o(A(N,C,G,\{X_n\})),$$

and since $0\le A(N,C,G,\{X_n\})\le N$, we conclude that

$$\lim_{N\to\infty}\frac{A(N,C,G,\{X_n\})}{N}=|\det G|^{-m}.$$

There will be several occasions to exploit relations to uniform distribution of sequences of lattice points. For this reason, we recall the relevant definitions as given by Niederreiter [**6**]. For a positive integer k, let $\mathbf{Z}^k$ be the set of k-dimensional lattice points. Let $\mathbf{m}=(m_1,\ldots,m_k)$ be a k-tuple of natural numbers. For elements $\mathbf{a}=(a_1,\ldots,a_k)$ and $\mathbf{b}=(b_1,\ldots,b_k)$ of $\mathbf{Z}^k$, we write $\mathbf{a}\equiv\mathbf{b}\bmod\mathbf{m}$ if $a_j\equiv b_j \bmod m_j$ for $1\le j\le k$. Given a sequence $\{\mathbf{x}_n\}$, $n=1,2,\ldots,$ of elements of $\mathbf{Z}^k$ and a positive integer N, let $A(N,\mathbf{b},\mathbf{m},\{\mathbf{x}_n\})$ denote the number of n, $1\le n\le N$, such that $\mathbf{x}_n\equiv\mathbf{b}\bmod\mathbf{m}$.

Definition 2.9. Let $\mathbf{m}=(m_1,\ldots,m_k)$ be a k-tuple of natural numbers. Then the sequence $\{\mathbf{x}_n\}$, $n=1,2,\ldots,$ of elements of $\mathbf{Z}^k$ is called *uniformly distributed modulo* $(m_1,\ldots,m_k)$ (abbreviated u.d. mod$(m_1,\ldots,m_k)$ or u.d. mod $\mathbf{m}$) if

$$\lim_{N\to\infty}\frac{A(N,\mathbf{b},\mathbf{m},\{\mathbf{x}_n\})}{N}=\frac{1}{m_1\ldots m_k}$$

holds for every $\mathbf{b}\in\mathbf{Z}^k$.

Definition 2.10. The sequence $\{\mathbf{x}_n\}$, $n=1,2,\ldots,$ of elements of $\mathbf{Z}^k$ is called *uniformly distributed in* $\mathbf{Z}^k$ (abbreviated u.d. in $\mathbf{Z}^k$) if it is u.d. mod $\mathbf{m}$ for all possible $\mathbf{m}$.

3. Uniform distribution modulo a left ideal. A standard criterion for uniform distribution is the Weyl criterion which, in a suitably general form, reads as follows (see [**2**, Chapter 4] for the proof and the definition of uniform distribution in a compact group).

Lemma 3.1. *Let H be a compact abelian group and $\hat{H}$ its character group. Then a sequence $\{h_n\}$, $n=1,2,\ldots,$ of elements of H is u.d. in H if and only if*

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}\chi(h_n)=0$$

for all nontrivial $\chi\in\hat{H}$.

For a nonsingular $G\in\mathrm{Mat}_m(\mathbf{Z})$, we write $\langle G\rangle$ for the principal left ideal generated by G and view $\mathrm{Mat}_m(\mathbf{Z})/\langle G\rangle$ as a compact additive abelian group in the discrete topology. A

https://doi.org/10.1017/S001708950000389X Published online by Cambridge University Press

sequence $\{X_n\}$ of elements of $\mathrm{Mat}_m(\mathbf{Z})$ is then u.d. mod G if and only if the sequence $\{X_n+\langle G\rangle\}$ is u.d. in $\mathrm{Mat}_m(\mathbf{Z})/\langle G\rangle$ in the sense referred to in Lemma 3.1. Therefore, in order to obtain an explicit version of the Weyl criterion for uniform distribution mod G, it is necessary to find a formula for the characters of $\mathrm{Mat}_m(\mathbf{Z})/\langle G\rangle$. As a matter of convenience, we describe these characters as functions on $\mathrm{Mat}_m(\mathbf{Z})$. Then, of course, we have to verify that the function values only depend on the residue class mod G. We write $\exp(x)=e^{2\pi ix}$ for real x and $\mathrm{tr}(C)$ for the trace of $C\in\mathrm{Mat}_m(\mathbf{Q})$, where $\mathbf{Q}$ is the field of rational numbers.

THEOREM 3.2. *Let* $G\in\mathrm{Mat}_m(\mathbf{Z})$ *be nonsingular, and let U and V be unimodular matrices such that UGV is a diagonal matrix, say* $UGV=\mathrm{diag}(g_1,\ldots,g_m)$. *Then the distinct characters of the group* $\mathrm{Mat}_m(\mathbf{Z})/\langle G\rangle$ *are given by*

$$\chi_R(A)=\exp(\mathrm{tr}(RAG^{-1}U^{-1})) \quad \textit{for} \quad A\in\mathrm{Mat}_m(\mathbf{Z}), \tag{3}$$

where $R=(r_{ij})\in\mathrm{Mat}_m(\mathbf{Z})$ *with* $0\le r_{ij}<|g_i|$ *for* $1\le i,j\le m$.

Proof. First of all, the functions χ_R are really functions on $\mathrm{Mat}_m(\mathbf{Z})/\langle G\rangle$ since one checks easily that $\chi_R(A)=\chi_R(B)$ whenever $A\equiv B$ mod G. Furthermore, for any $A,B\in\mathrm{Mat}_m(\mathbf{Z})$ one has $\chi_R(A+B)=\chi_R(A)\chi_R(B)$. To complete the proof, we note that the abelian group $\mathrm{Mat}_m(\mathbf{Z})/\langle G\rangle$ of order $|\det G|^m$ has $|\det G|^m$ characters, so that it suffices to show that the $|\det G|^m$ characters χ_R given by (3) are distinct. Suppose that $x_R=\chi_S$, where $R=(r_{ij})$, $S=(s_{ij})$ with $0\le r_{ij}, s_{ij}<|g_i|$ for $1\le i,j\le m$. Let E_{ji} be the $m\times m$ matrix having 1 in the (j,i) entry and 0 elsewhere. Then $\chi_R(E_{ji}V^{-1})=\exp(r_{ij}g_i^{-1})$ and $\chi_S(E_{ji}V^{-1})=\exp(s_{ij}g_i^{-1})$, and so g_i divides $r_{ij}-s_{ij}$. But $-|g_i|<r_{ij}-s_{ij}<|g_i|$, hence $r_{ij}=s_{ij}$ for $1\le i,j\le m$, that is, $R=S$.

THEOREM 3.3. (Weyl Criterion). *Let* $G\in\mathrm{Mat}_m(\mathbf{Z})$ *be nonsingular, and let U and V be unimodular matrices such that UGV is a diagonal matrix, say* $UGV=\mathrm{diag}(g_1,\ldots,g_m)$. *Then the sequence $\{X_n\}$ of elements of* $\mathrm{Mat}_m(\mathbf{Z})$ *is u.d.* mod G *if and only if*

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}\exp(\mathrm{tr}(RX_nG^{-1}U^{-1}))=0$$

holds for all $R=(r_{ij})\in\mathrm{Mat}_m(\mathbf{Z})$ *with* $R\neq0$ *and* $0\le r_{ij}<|g_i|$ *for* $1\le i,j\le m$.

Proof. This follows from Lemma 3.1 and Theorem 3.2.

The character formula (3) can also be used to investigate the relationship between distribution properties modulo different left ideals. First we note a simple result in this direction.

THEOREM 3.4. *Let* $F,G\in\mathrm{Mat}_m(\mathbf{Z})$*with F nonsingular and* $F\in\langle G\rangle$. *Then a sequence of elements of* $\mathrm{Mat}_m(\mathbf{Z})$ *is u.d.* mod G *whenever it is u.d.* mod F.

https://doi.org/10.1017/S001708950000389X Published online by Cambridge University Press

Proof. Let $\{X_n\}$ be a u.d. sequence mod F and $B\in \mathrm{Mat}_m(\mathbf{Z})$. Then

$$A(N,B,G,\{X_n\})=\sum A(N,C,F,\{X_n\}),$$

where the summation is taken over all distinct cosets $C+\langle F\rangle$ such that $C\equiv B \bmod G$. There are $|\det F|^m\,|\det G|^{-m}$ such cosets. It follows that

$$\begin{aligned}\lim_{N\to\infty}\frac{A(N,B,G,\{X_n\})}{N}&=\lim_{N\to\infty}\frac{1}{N}\sum A(N,C,F,\{X_n\})\\&=\frac{|\det F|^m}{|\det G|^m}\cdot\frac{1}{|\det F|^m}\\&=\frac{1}{|\det G|^m},\end{aligned}$$

and so $\{X_n\}$ is u.d. mod G.

THEOREM 3.5. *Let $\mathscr{F}$ be a nonempty set of nonsingular matrices in* $\mathrm{Mat}_m(\mathbf{Z})$ *and let $\mathscr{G}=\{G\in\mathrm{Mat}_m(\mathbf{Z}):G$ nonsingular, $F\notin\langle G\rangle$ for all $F\in\mathscr{F}\}$. Then there exists a sequence of elements of* $\mathrm{Mat}_m(\mathbf{Z})$ *which is u.d.* mod F *for all $F\in\mathscr{F}$ and, for each $G\in\mathscr{G}$, is not u.d.* mod G.

Proof. We apply the following theorem of Zame [**11**]. Let H be a locally compact abelian group with countable base, and let $\mathscr{S}\neq\varnothing$ and $\mathscr{T}$ be countable collections of closed subgroups of H such that: (i) finite intersections of elements of $\mathscr{S}\cup\mathscr{T}$ are of compact index; (ii) for each $S\in\mathscr{S}$ and $T\in\mathscr{T}$, we have $S\not\subseteq T$; (iii) for each $T\in\mathscr{T}$, there exists a character χ_T of H such that χ_T is trivial on T but is nontrivial on each $S\in\mathscr{S}$. Then there exists a sequence of elements of H which is u.d. mod S for all $S\in\mathscr{S}$ and, for each $T\in\mathscr{T}$, is not u.d. mod T. Now let $H=\mathrm{Mat}_m(\mathbf{Z})$ with the discrete topology, $\mathscr{S}=\{\langle F\rangle:F\in\mathscr{F}\}$, and $\mathscr{T}=\{\langle G\rangle:G\in\mathscr{G}\}$. Then conditions (i) and (ii) are easily checked (note that every principal left ideal generated by a nonsingular matrix has finite, thus compact, index). As to condition (iii), let $\langle G\rangle\in\mathscr{T}$ be given and choose $R=I_m$, the $m\times m$ identity matrix, in the character formula (3). This character χ is trivial on $\langle G\rangle$. For $F\in\mathscr{F}$ let $FG^{-1}U^{-1}=(a_{ij})$, where U, V are unimodular such that UGV is a diagonal matrix. Since $F\notin\langle G\rangle$, we have $FG^{-1}\notin\mathrm{Mat}_m(\mathbf{Z})$, and so $FG^{-1}U^{-1}\notin\mathrm{Mat}_m(\mathbf{Z})$. Then some $a_{i_0j_0}\notin\mathbf{Z}$, hence $\chi(E_{j_0i_0}F)=\exp(a_{i_0j_0})\neq 1$. Therefore χ is nontrivial on $\langle F\rangle$. Thus χ satisfies the properties in (iii), and the theorem follows.

We consider now the connection between uniform distribution mod G of sequences of elements of $\mathrm{Mat}_m(\mathbf{Z})$ and uniform distribution of sequences of lattice points.

THEOREM 3.6. *Let $G\in\mathrm{Mat}_m(\mathbf{Z})$ be nonsingular, and let U and V be unimodular matrices such that UGV is a diagonal matrix, say $UGV=\mathrm{diag}(g_1,\dots,g_m)$. If $\{X_n\}$ is a sequence of elements of* $\mathrm{Mat}_m(\mathbf{Z})$ *with $X_nV=(x_{ij}^{(n)})$ for $n=1,2,\dots$, then $\{X_n\}$ is u.d.* mod G *if and only if the sequence $\{(x_{11}^{(n)},\dots,x_{1m}^{(n)},x_{21}^{(n)},\dots,x_{2m}^{(n)},\dots,x_{m1}^{(n)},\dots,x_{mm}^{(n)})\}$,*

https://doi.org/10.1017/S001708950000389X Published online by Cambridge University Press

$n = 1, 2, \ldots,$ of elements of $\mathbf{Z}^{m^2}$ *is u.d.* mod $(|g_1|, \ldots, |g_m|, |g_1|, \ldots, |g_m|, \ldots, |g_1|, \ldots, |g_m|)$.

Proof. For any matrix $A = (a_{ij}) \in \mathrm{Mat}_m(\mathbf{Z})$, let $\psi(A)$ denote the lattice point $(a_{11}, \ldots, a_{1m}, \; a_{21}, \ldots, a_{2m}, \ldots, a_{m1}, \ldots, a_{mm}) \in \mathbf{Z}^{m^2}$. Put $\mathbf{g} = (|g_1|, \ldots, |g_m|, |g_1|, \ldots, |g_m|, \ldots, |g_1|, \ldots, |g_m|) \in \mathbf{Z}^{m^2}$. Then $A(N, B, \mathrm{diag}(g_1, \ldots, g_m), \{X_n\}) = A(N, \psi(B), \mathbf{g}, \{\psi(X_n)\})$ for any $B \in \mathrm{Mat}_m(\mathbf{Z})$. This implies that the sequence $\{\psi(X_n V)\}$ is u.d. mod $\mathbf{g}$ if and only if $\{X_n V\}$ is u.d. mod $\mathrm{diag}(g_1, \ldots, g_m)$. The latter is equivalent to $\{X_n\}$ being u.d. mod G, because of Lemma 2.7(iii).

We obtain an alternative form of the Weyl criterion for uniform distribution mod G if we use the criterion in Theorem 3.6 together with the Weyl criterion for uniform distribution mod $\mathbf{g}$ (see Niederreiter [**6**, Theorem 2.1]).

THEOREM 3.7 (Weyl criterion). *With the notation of Theorem* 3.6, *the sequence* $\{X_n\}$ *is u.d.* mod G *if and only if*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \exp\left(\sum_{i=1}^{m} \sum_{j=1}^{m} \frac{r_{ij} x_{ij}^{(n)}}{|g_j|} \right) = 0$$

holds for all $R = (r_{ij}) \in \mathrm{Mat}_m(\mathbf{Z})$ *with* $R \neq 0$ *and* $0 \leq r_{ij} < |g_j|$ *for* $1 \leq i, j \leq m$.

Once the connection with uniform distribution of sequences of lattice points is established, other criteria for uniform distribution mod G can be obtained, for instance by combining Theorem 3.6 above with Theorem 4.8 in Niederreiter and Lo [**7**].

For certain rings, such as rings of algebraic integers, there exist elements for which suitable integral multiples form a sequence which is uniformly distributed modulo a nontrivial left ideal (see Niederreiter and Lo [**7**, §4]). It is interesting to note that, apart from the case $m = 1$, this cannot happen for $\mathrm{Mat}_m(\mathbf{Z})$.

THEOREM 3.8. *Let* $G \in \mathrm{Mat}_m(\mathbf{Z})$, *where* $|\det G| \geq 2$ *and* $m \geq 2$. *Then no sequence of the form* $\{x_n A\}$ *with* $\{x_n\}$ *being a sequence of rational integers and* $A \in \mathrm{Mat}_m(\mathbf{Z})$ *can be u.d.* mod G.

Proof. Suppose $\{x_n A\}$ were u.d. mod G. Let U and V be unimodular matrices such that UGV is a diagonal matrix $D = \mathrm{diag}(g_1, \ldots, g_m)$. Then $\{x_n AV\}$ is u.d. mod D by Lemma 2.7.(iii). Setting $AV = B$, we note that $\{x_n B\}$ must contain elements from every residue class mod D, and so the additive group $\mathrm{Mat}_m(\mathbf{Z})/\langle D\rangle$ is cyclic with generator $B + \langle D\rangle$. It is easily checked that $C = (c_{ij}) \in \mathrm{Mat}_m(\mathbf{Z})$ is $\equiv 0 \bmod D$ if and only if $c_{ij} \equiv 0 \bmod |g_j|$ for $1 \leq i, j \leq m$. Now for the matrix B we have $|\det G|\, B = |g_1 \ldots g_m|\, B \equiv 0 \bmod D$, and so the order of $B + \langle D\rangle$ in $\mathrm{Mat}_m(\mathbf{Z})/\langle D\rangle$ is at most $|\det G|$, which is less than $|\det G|^m = |\det D|^m$, the order of $\mathrm{Mat}_m(\mathbf{Z})/\langle D\rangle$. Thus $B + \langle D\rangle$ cannot be a generator, and we have arrived at a contradiction.

4. Uniform distribution in $\mathrm{Mat}_m(\mathbf{Z})$. The following auxiliary result is useful when checking uniform distribution in $\mathrm{Mat}_m(\mathbf{Z})$.

https://doi.org/10.1017/S001708950000389X Published online by Cambridge University Press

Lemma 4.1. *Let s be a given positive integer. Then the sequence $\{X_n\}$ of elements of* $\mathrm{Mat}_m(\mathbf{Z})$ *is u.d. in* $\mathrm{Mat}_m(\mathbf{Z})$ *if and only if $\{X_n\}$ is u.d.* mod tsI_m *for all positive integers t, where I_m is the $m \times m$ identity matrix.*

Proof. The condition is certainly necessary. As to sufficiency, let $G \in \mathrm{Mat}_m(\mathbf{Z})$ be nonsingular. Then $\{X_n\}$ is u.d. mod $|\det G|\, sI_m$, and so u.d. mod G by Theorem 3.4 and the fact that $(\det G)I_m = G^*G$, where $G^* \in \mathrm{Mat}_m(\mathbf{Z})$ is the transpose of the matrix of cofactors of G. Since G is an arbitrary nonsingular matrix, $\{X_n\}$ is u.d. in $\mathrm{Mat}_m(\mathbf{Z})$.

Theorem 4.2. (Weyl Criterion). *The sequence $\{X_n\}$ of elements of* $\mathrm{Mat}_m(\mathbf{Z})$ *is u.d. in* $\mathrm{Mat}_m(\mathbf{Z})$ *if and only if*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \exp(\operatorname{tr}(PX_n)) = 0$$

holds for all $P \in \mathrm{Mat}_m(\mathbf{Q})$ with $P \notin \mathrm{Mat}_m(\mathbf{Z})$.

Proof. To show the necessity, we choose P as above. Then there exists a positive integer d such that $Q = dP \in \mathrm{Mat}_m(\mathbf{Z})$, where not all entries of Q are divisible by d. We write $Q = dA + R$ with A, $R \in \mathrm{Mat}_m(\mathbf{Z})$ and $R = (r_{ij})$ with $0 \le r_{ij} < d$ for $1 \le i, j \le m$ and $R \ne 0$. Since $\{X_n\}$ is u.d. in $\mathrm{Mat}_m(\mathbf{Z})$, the sequence is u.d. mod dI_m, and so

$$\begin{aligned}
\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \exp(\operatorname{tr}(PX_n)) &= \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \exp\left(\operatorname{tr}\left(\frac{1}{d} RX_n\right)\right) \\
&= \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \exp(\operatorname{tr}(RX_n(dI_m)^{-1})) \\
&= 0
\end{aligned}$$

by Theorem 3.3.

Conversely, suppose the condition of the theorem is satisfied. According to Lemma 4.1 it suffices to show that $\{X_n\}$ is u.d. mod tI_m for all positive integers t. Such a t being chosen, we note that because of Theorem 3.3 it remains to prove that

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \exp\left(\operatorname{tr}\left(\frac{1}{t} RX_n\right)\right) = 0$$

holds for all $R = (r_{ij}) \in \mathrm{Mat}_m(\mathbf{Z})$ with $R \ne 0$ and $0 \le r_{ij} < t$ for $1 \le i, j \le m$. However, this follows from the given condition with $P = (1/t)R$.

The above criterion can be used to reduce the question of uniform distribution in $\mathrm{Mat}_m(\mathbf{Z})$ to one of uniform distribution of sequences of rational integers.

Theorem 4.3. *The sequence $\{X_n\}$ of elements of* $\mathrm{Mat}_m(\mathbf{Z})$ *is u.d. in* $\mathrm{Mat}_m(\mathbf{Z})$ *if and only if for all $B \in \mathrm{Mat}_m(\mathbf{Z})$ with relatively prime entries the sequence* $\{\operatorname{tr}(BX_n)\}$ *is u.d. in* $\mathbf{Z}$.

https://doi.org/10.1017/S001708950000389X Published online by Cambridge University Press

Proof. Suppose $\{X_n\}$ is u.d. in $\mathrm{Mat}_m(\mathbf{Z})$, and take $B \in \mathrm{Mat}_m(\mathbf{Z})$ with relatively prime entries. We have to show that for every integer $s \geq 2$ the sequence $\{\mathrm{tr}(BX_n)\}$ is u.d. mod s. Let j be an arbitrary integer with $1 \leq j < s$. Then we can write $j/s = q/r$, where q and r are relatively prime integers with $r > 1$. the matrix $P = (q/r)B$ is then in $\mathrm{Mat}_m(\mathbf{Q})$, but not in $\mathrm{Mat}_m(\mathbf{Z})$ because of the condition on B. It follows from Theorem 4.2 that

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \exp\left(\frac{i}{s}\,\mathrm{tr}(BX_n)\right) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \exp\left(\mathrm{tr}\left(\frac{q}{r}\,BX_n\right)\right) = 0,$$

and so $\{\mathrm{tr}(BX_n)\}$ is u.d. mod s by [**2**, p. 306, Theorem 1.2].

To show the sufficiency, take $P \in \mathrm{Mat}_m(\mathbf{Q})$ with $P \notin \mathrm{Mat}_m(\mathbf{Z})$. If s is the least common denominator of the entries of P, then $s > 1$. We can write $P = (1/s)B$ with $B \in \mathrm{Mat}_m(\mathbf{Z})$ having relatively prime entries. Since $\{\mathrm{tr}(BX_n)\}$ is u.d. mod s by assumption, we get

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \exp(\mathrm{tr}(PX_n)) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \exp\left(\frac{1}{s}\,\mathrm{tr}(BX_n)\right) = 0$$

because of [**2**, p. 306, Theorem 1.2]. Thus, according to Theorem 4.2, the sequence $\{X_n\}$ is u.d. in $\mathrm{Mat}_m(\mathbf{Z})$.

The connection between uniform distribution of sequences of matrices and uniform distribution of sequences of lattice points, already used in the previous section, can be exploited further. Let ψ be the mapping defined in the proof of Theorem 3.6, i.e., $\psi(A) = (a_{11}, \ldots, a_{1m}, a_{21}, \ldots, a_{2m}, \ldots, a_{m1}, \ldots, a_{mm}) \in \mathbf{Z}^{m^2}$ for $A = (a_{ij}) \in \mathrm{Mat}_m(\mathbf{Z})$.

THEOREM 4.4. *The sequence* $\{X_n\}$ *of elements of* $\mathrm{Mat}_m(\mathbf{Z})$ *is u.d. in* $\mathrm{Mat}_m(\mathbf{Z})$ *if and only if the sequence* $\{\psi(X_n)\}$ *is u.d. in* $\mathbf{Z}^{m^2}$.

Proof. We first show the necessity of the condition. Since $\{X_n\}$ is u.d. in $\mathrm{Mat}_m(\mathbf{Z})$, the sequence is, in particular, u.d. mod sI_m, where s is an arbitrary positive integer. Then Theorem 3.6 implies that $\{\psi(X_n)\}$ is u.d. mod$(s, s, \ldots, s)$, and so by Niederreiter [**6**, Theorem 2.4] the sequence $\{\psi(X_n)\}$ is u.d. in $\mathbf{Z}^{m^2}$.

As to the sufficiency, if $\{\psi(X_n)\}$ is u.d. in $\mathbf{Z}^{m^2}$, then $\{\psi(X_n)\}$ is u.d. mod$(t, t, \ldots, t)$ for any positive integer t, and so Theorem 3.6 implies that $\{X_n\}$ is u.d. mod tI_m for any positive integer t. It follows from Lemma 4.1 that $\{X_n\}$ is u.d. in $\mathrm{Mat}_m(\mathbf{Z})$.

An alternative version of the Weyl criterion can be based on Theorem 4.4. If $\mathbf{a} = (a_1, \ldots, a_{m^2})$ and $\mathbf{b} = (b_1, \ldots, b_{m^2})$ are two vectors of the euclidean space $\mathbf{R}^{m^2}$, then $\mathbf{a}\cdot\mathbf{b} = \sum_{i=1}^{m^2} a_i b_i$ denotes their standard inner product.

THEOREM 4.5. (Weyl Criterion). *The sequence* $\{X_n\}$ *of elements of* $\mathrm{Mat}_m(\mathbf{Z})$ *is u.d. in* $\mathrm{Mat}_m(\mathbf{Z})$ *if and only if*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \exp(\mathbf{r}\cdot\psi(X_n)) = 0$$

for all $\mathbf{r} = (r_1, \ldots, r_{m^2})$ *with all* r_i *being rationals, but not all* r_i *being integers.*

Proof. This follows from Theorem 4.4 and the Weyl criterion for uniform distribution in $\mathbf{Z}^{m^2}$ given by Niederreiter [**6**, Theorem 2.2].

EXAMPLES 4.6. (i) If the real numbers 1, $\alpha_{11}, \ldots, \alpha_{1m}, \alpha_{21}, \ldots, \alpha_{2m}, \ldots, \alpha_{m1}, \ldots, \alpha_{mm}$ are linearly independent over the rationals, then the sequence $\{([n\alpha_{ij}])\}$, $n = 1, 2, \ldots,$ is u.d. in $\mathrm{Mat}_m(\mathbf{Z})$, where $[t]$ denotes the integral part of $t \in \mathbf{R}$. This follows from Theorem 4.4 and a result of Niederreiter [**6**, p. 480].

(ii) The elements of $\mathrm{Mat}_m(\mathbf{Z})$ can be arranged into a u.d. sequence in $\mathrm{Mat}_m(\mathbf{Z})$. This is achieved by first employing the so-called cube method of Lo and Niederreiter [**4**, § 3] to arrange all elements of $\mathbf{Z}^{m^2}$ into a u.d. sequence in $\mathbf{Z}^{m^2}$, which is possible by [**4**, Theorem 3.3], and then applying the inverse of the mapping ψ to get a sequence containing all elements of $\mathrm{Mat}_m(\mathbf{Z})$ without repetition. This sequence is u.d. in $\mathrm{Mat}_m(\mathbf{Z})$ by Theorem 4.4.

The second example above raises the question of characterizing those subsets of $\mathrm{Mat}_m(\mathbf{Z})$ whose elements can be arranged into a u.d. sequence in $\mathrm{Mat}_m(\mathbf{Z})$. This is settled by the following result.

THEOREM 4.7. *The elements of the subset $\mathscr{E}$ of* $\mathrm{Mat}_m(\mathbf{Z})$ *can be arranged into a u.d. sequence in* $\mathrm{Mat}_m(\mathbf{Z})$ *if and only if every coset of every left ideal $\langle G\rangle$ with $G = \mathrm{Mat}_m(\mathbf{Z})$ nonsingular contains at least one element of $\mathscr{E}$.*

Proof. The condition is obviously necessary. To prove the sufficiency, we transfer the problem into a suitable setting. Let K be an algebraic number field of degree m^2 over $\mathbf{Q}$ and let $\mathcal{O}$ be the ring of algebraic integers in K. Furthermore, let $\omega_1, \omega_2, \ldots, \omega_{m^2}$ be an integral basis for $\mathcal{O}$. We set up an injective mapping τ from $\mathrm{Mat}_m(\mathbf{Z})$ onto $\mathcal{O}$ by putting

$$\tau(A) = \sum_{i,j=1}^{m} a_{ij}\omega_{(i-1)m+j}$$

for $A = (a_{ij}) \in \mathrm{Mat}_m(\mathbf{Z})$. We claim that $\tau(\mathscr{E})$ has the property that every coset of every nonzero integral ideal of $\mathcal{O}$ contains an element of $\tau(\mathscr{E})$. To see this, let J be a nonzero integral ideal of $\mathcal{O}$ and consider a coset $\beta + J$ with $\beta \in \mathcal{O}$. Let h be a positive integer with $h \in J$, e.g., h can be taken to be the norm of J. Let $B \in \mathrm{Mat}_m(\mathbf{Z})$ be such that $\tau(B) = \beta$. By the condition on $\mathscr{E}$, there exists an $E \in \mathscr{E}$ with $E \equiv B \bmod hI_m$. One checks easily that this implies $\tau(E) \equiv \beta \bmod h\mathcal{O}$, and so $\tau(E) \in \beta + J$. Thus $\tau(\mathscr{E})$ has the property claimed above. It follows then from [**4**, Theorem 4.5] and [**7**, Theorem 3.9] that the elements of $\tau(\mathscr{E})$ can be arranged into a u.d. sequence in $\mathcal{O}$, say $\{\tau(E_n)\}$ with $E_n \in \mathscr{E}$ for $n = 1, 2, \ldots$. However, by combining Theorem 4.4 with a remark from [**4**, p. 193], one obtains that a sequence $\{X_n\}$ of elements of $\mathrm{Mat}_m(\mathbf{Z})$ is u.d. in $\mathrm{Mat}_m(\mathbf{Z})$ if and only if $\{\tau(X_n)\}$ is u.d. in $\mathcal{O}$. Consequently, the sequence $\{E_n\}$ is u.d. in $\mathrm{Mat}_m(\mathbf{Z})$ and is therefore the desired sequential arrangement of the elements of $\mathscr{E}$.

COROLLARY 4.8. *The nonsingular matrices in* $\mathrm{Mat}_m(\mathbf{Z})$ *can be arranged into a u.d. sequence in* $\mathrm{Mat}_m(\mathbf{Z})$.

https://doi.org/10.1017/S001708950000389X Published online by Cambridge University Press

Proof. It suffices to show that the set $\mathscr{C}$ of nonsingular matrices in $\mathrm{Mat}_m(\mathbf{Z})$ satisfies the condition of Theorem 4.7. Let $B+\langle G\rangle$ be a coset with $B, G\in \mathrm{Mat}_m(\mathbf{Z})$ and G nonsingular. Choose an integer t which is not an eigenvalue of BG^{-1}. Then $B-tG=(BG^{-1}-tI_m)G$ is a nonsingular matrix contained in $B+\langle G\rangle$.

On the other hand, it is clear that the unimodular matrices in $\mathrm{Mat}_m(\mathbf{Z})$ cannot be arranged into a u.d. sequence in $\mathrm{Mat}_m(\mathbf{Z})$ since there is no unimodular $U\in \mathrm{Mat}_m(\mathbf{Z})$ with $U\equiv 0 \bmod 2I_m$.

REFERENCES

1. L. Gotusso, Successioni uniformemente distribuite in corpi finiti, *Atti Sem. Mat. Fis. Univ. Modena* **12** (1962/63), 215–232.

2. L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences* (Wiley-Interscience, 1974).

3. L. Kuipers, H. Niederreiter and J.-S. Shiue, Uniform distribution of sequences in the ring of Gaussian integers, *Bull. Inst. Math. Acad. Sinica* **3** (1975), 311–325.

4. S. K. Lo and H. Niederreiter, Banach-Buck measure, density, and uniform distribution in rings of algebraic integers, *Pacific J. Math.* **61** (1975), 191–208.

5. M. Newman, *Integral Matrices* (Academic Press, 1972).

6. H. Niederreiter, On a class of sequences of lattice points, *J. Number Theory* **4** (1972), 477–502.

7. H. Niederreiter and S. K. Lo, Uniform distribution of sequences of algebraic integers, *Math. J. Okayama Univ.* **18** (1975), 13–29.

8. H. Niederreiter and J.-S. Shiue, Equidistribution of linear recurring sequences in finite fields, *Indagationes Math.* **80** (1977), 397–405.

9. I. Niven, Uniform distribution of sequences of integers, *Trans. Amer. Math. Soc.* **98** (1961), 52–61.

10. J.-S. Shiue and C.-P. Hwang, Complete residue systems in the ring of matrices of rational integers, *International J. of Math. and Math. Sci.* **1** (1978), 217–225.

11. A. Zame, On a problem of Narkiewicz concerning uniform distributions of sequences of integers, *Colloq. Math.* **24** (1972), 271–273.

UNIVERSITY OF THE WEST INDIES
KINGSTON 7
JAMAICA

NATIONAL CHENGCHI UNIVERSITY
TAIPEI
TAIWAN
and
UNIVERSITY OF SOUTH FLORIDA
TAMPA
FLORIDA 33620
USA

https://doi.org/10.1017/S001708950000389X Published online by Cambridge University Press